Study evaluating the status quo and the legal implications of third party liability for the European security industry

Editors:

Lucas Bergkamp
Michael Faure
Monika Hinteregger
Niels Philipsen

Submitted to: European Commission / DG ENTR

Final Report, Maastricht, 11 October 2013
Contributors:

Anke van Bergeijk (Hunton & Williams)
Lucas Bergkamp (Hunton & Williams)
Michael Faure (METRO, Maastricht University)
Nicolas Herbatschek (Hunton & Williams)
Monika Hinteregger (University of Graz and ECTIL)
Jing Liu (METRO, Maastricht University)
Maida Oringher Lerner (Hunton & Williams)
Niels Philipsen (METRO, Maastricht University)
Mehdi Piri (METRO, Maastricht University)
Kristel de Smedt (METRO, Maastricht University)
Evan D. Wolff (Hunton & Williams)

Country reporters:

Ewa Baginska (Nicolaus Copernicus University)
Willem van Boom (Erasmus University Rotterdam)
Florence G’sell Macrez (Université de Bretagne Occidentale)
Siewert Lindenbergh (Erasmus University Rotterdam)
Claire Mc Ivor (University of Birmingham)
Philip Mielnicki (Stockholm University)
Pedro del Olmo (University Carlos III of Madrid)
Peter Rott (University of Copenhagen)
Marten Schultz (Stockholm University)
# Table of Contents

List of Abbreviations .......................................................................................................................... xiii

Executive Summary .............................................................................................................................. xv

1. Introduction and background ............................................................................................................ xv
2. Definition of security industry and methodology .............................................................................. xv
3. Analysis of comparable EU legislation and related case law and potential analogy-bearing international law treaties ............................................................................................................. xvi
4. Analysis of comparable EU-Member States legislation and related case law .................................... xvii
5. Analysis of the US Safety Act and liability system ............................................................................. xviii
7. Conclusions ......................................................................................................................................... xx

Chapter 1 Introduction .......................................................................................................................... 1

1.1. Background ...................................................................................................................................... 1
1.1.1. Increasing exposure to risks ........................................................................................................... 1
1.1.2. … leads to a new security industry ............................................................................................... 1
1.1.3. Need for a clear liability regime .................................................................................................. 2
1.2. Goals .............................................................................................................................................. 2
1.3. A few starting points ....................................................................................................................... 3
1.4. Methodology ................................................................................................................................... 3
1.4.1. Three methodological approaches ............................................................................................. 3
1.4.1.1. Legal analysis .......................................................................................................................... 3
1.4.1.2. Law and economics ............................................................................................................... 4
1.4.1.3. Empirics .................................................................................................................................. 5
1.4.2. Checklist .................................................................................................................................... 5
1.5. Structure ......................................................................................................................................... 5

Chapter 2 A definition of the security industry in Europe ...................................................................... 7

2.1. Introduction ...................................................................................................................................... 7
2.2. A definition of the security industry in Europe ............................................................................... 7
2.3. A conceptual definition of the security industry ............................................................................. 8
2.4. What are the security challenges perceived by stakeholders/ EU citizens? ................................. 8
2.5. Main tasks of the security industry ............................................................................................... 11
2.6. Who is the security industry? ......................................................................................................... 11
2.6.1. Difficulty to limit the definition of the security industry ............................................................ 11
2.6.2. Who does belong to the security industry? ............................................................................... 12
2.6.3. Fuzzy boundaries ...................................................................................................................... 14
2.6.4. Closely related industries and markets ...................................................................................... 15
2.6.5. Comparison with the US .......................................................................................................... 15
2.7. Conclusion ................................................................................................................................... 16

Chapter 3 Analysis of comparable EU legislation ................................................................................ 19

3.1.1. Brief summary of the regime ...................................................................................................... 19
3.1.2. Basis of liability ........................................................................................................................... 20
3.1.3. Liable persons (attribution of liability) ......................................................................................... 20
3.1.4. Damage covered .......................................................................................................................... 22
3.1.5. Exclusions and defences ............................................................................................................. 22
## 3.1.6. Causation ................................................................. 24
## 3.1.7. Relation with (other) regulation .................................. 25
## 3.1.8. Financial security and compensation mechanisms .............. 25
## 3.1.9. Rules of evidence ..................................................... 26
## 3.1.10. Jurisdictional and procedural issues ............................... 26
## 3.1.11. Conclusions Environmental Liability Directive .................. 26
## 3.2. Legal analysis of product-related EU legislation .................... 27
### 3.2.1.1. Brief summary of the regime .................................... 28
## 3.2.1.2. Basis of liability .................................................. 29
## 3.2.1.3. Liable persons (attribution of liability) .......................... 30
## 3.2.1.4. Damage covered ................................................... 31
## 3.2.1.5. Exclusions and defences ......................................... 31
## 3.2.1.6. Causation .......................................................... 32
## 3.2.1.7. Relation with regulation ......................................... 33
## 3.2.1.8. Financial security and compensation mechanisms ............. 33
## 3.2.1.9. Rules of evidence .................................................. 33
## 3.2.1.10. Jurisdictional and procedural issues ............................. 33
## 3.2.1.11. Applicability in time ............................................ 34
## 3.2.1.12. Conclusions Product Liability Directive ...................... 34
## 3.2.2. General Product Safety Directive 2001/95 .......................... 34
### 3.2.2.1. Brief summary of the regime .................................... 34
## 3.2.2.2. Key Objectives .................................................... 35
## 3.2.2.3. Key Instruments .................................................. 35
## 3.2.2.4. Regulated entities, activities and products ...................... 36
## 3.2.2.5. Relation with liability ............................................ 37
## 3.2.2.6. Financial security and compensation mechanisms ............... 38
## 3.2.2.7. Applicability in time ............................................. 38
## 3.2.2.8. Other relevant features .......................................... 38
## 3.2.2.9. Conclusions Product Safety Directive and Implications for Security Industry ........................................ 39
## 3.2.3. REACH Regulation 1907/2006 and CLP Regulation 1272/2008 .................. 39
### 3.2.3.1. Brief summary of the regime .................................... 39
## 3.2.3.2. Key Objectives .................................................... 40
## 3.2.3.3. Key Instruments .................................................. 40
## 3.2.3.4. Regulated entities, activities and products ...................... 42
## 3.2.3.5. Relation with liability ............................................ 42
## 3.2.3.6. Financial security and compensation mechanisms ............... 43
## 3.2.3.7. Application in time .............................................. 43
## 3.2.3.8. Other relevant features .......................................... 44
## 3.2.3.9. Conclusions REACH and implications for security industry .......... 44
## 3.2.4. Plant Protection Product Regulation 1107/2009 .................... 45
### 3.2.4.1. Brief summary of the regime .................................... 45
## 3.2.4.2. Key Objectives .................................................... 45
## 3.2.4.3. Key Instruments .................................................. 45
## 3.2.4.4. Regulated entities, activities and products ...................... 45
## 3.2.4.5. Relation with liability ............................................ 46
## 3.2.4.6. Financial security and compensation mechanisms ............... 46
## 3.2.4.7. Application in time .............................................. 46
## 3.2.4.8. Other relevant features .......................................... 46
## 3.2.4.9. Conclusions Plant Protection Product Regulation and implications for security industry ........................................ 47
## 3.2.5. EUDRALEX ............................................................. 47
### 3.2.5.1. Brief summary of the regime .................................... 47
## 3.2.5.2. Key Objectives .................................................... 47
## 3.2.5.3. Key Instruments .................................................. 47
3.4.7. Relation with regulation ........................................................................................................... 66
3.4.8. Financial security and compensation mechanisms ............................................................... 67
3.4.9. Rules of evidence ......................................................................................................................... 67
3.4.10. Jurisdictional and procedural issues ....................................................................................... 67
3.4.11. Conclusions Auditor’s Liability and implications for security industry .................... 68
3.5. Legal Analysis of Further Secondary European Law .................................................................. 69
3.5.1. Regulation 44/2001 on the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) ........................................... 70
  3.5.1.1. Brief summary of the regime ................................................................................................ 70
  3.5.1.2. Applicability in time .............................................................................................................. 71
  3.5.1.3. Conclusions Regulation 44/2001 and relevance to the security industry .................... 72
3.5.2. Regulation 2201/2003 on the jurisdiction and the recognition and enforcement of judgments in matrimonial matters and matters of parental responsibility (Brussels II) .................................................................................................................... 72
  3.5.2.1. Brief summary of the regime ............................................................................................... 72
  3.5.2.2. Applicability in time .............................................................................................................. 73
  3.5.2.3. Conclusions Regulation 2201/2003 and relevance to the security industry .......... 73
3.5.3. Regulation 1393/2007 on the service of judicial and extrajudicial documents .......... 73
  3.5.3.1. Brief summary of the regime ............................................................................................... 73
  3.5.3.2. Applicability in time .............................................................................................................. 74
  3.5.3.3. Conclusions Regulation 1393/2007 and relevance to the security industry .......... 74
3.5.4. Regulation 1206/2001 on cooperation in the taking of evidence ........................................ 74
  3.5.4.1. Brief summary of the regime ............................................................................................... 74
  3.5.4.2. Applicability in time .............................................................................................................. 74
  3.5.4.3. Conclusions Regulation 1206/2001 and relevance to the security industry ........ 74
3.5.5. Decision 2001/470/EC on a European Judicial Network ...................................................... 75
  3.5.5.1. Brief summary of the regime ............................................................................................... 75
  3.5.5.2. Applicability in time .............................................................................................................. 75
  3.5.5.3. Conclusions Decision 2001/470 and relevance to the security industry .......... 75
3.5.6. Regulation 861/2007 on a European small claims procedure ............................................. 75
  3.5.6.1. Brief summary of the regime ............................................................................................... 75
  3.5.6.2. Applicability in time .............................................................................................................. 76
  3.5.6.3. Conclusions Regulation 861/2007 and relevance to the security industry .......... 76
3.5.7. Regulation 1896/2006 on a European order for payment procedure .................................... 76
  3.5.7.1. Brief summary of the regime ............................................................................................... 76
  3.5.7.2. Applicability in time .............................................................................................................. 76
  3.5.7.3. Conclusions Regulation 1896/2006 and relevance to the security industry .......... 77
3.5.8. Regulation 805/2004 on European enforcement order for uncontested claims .................... 77
  3.5.8.1. Brief summary of the regime ............................................................................................... 77
  3.5.8.2. Applicability in time .............................................................................................................. 77
  3.5.8.3. Conclusions Regulation 805/2004 and relevance to the security industry .......... 77
3.5.9. Directive 2008/52/EC on mediation ......................................................................................... 77
  3.5.9.1. Brief summary of the regime ............................................................................................... 77
  3.5.9.2. Applicability in time .............................................................................................................. 78
  3.5.9.3. Conclusions Mediation Directive and relevance to the security industry .......... 78
3.5.10. Directive 2003/8/EC on legal aid .......................................................................................... 78
  3.5.10.1. Brief summary of the regime ............................................................................................. 78
  3.5.10.2. Applicability in time ............................................................................................................ 78
  3.5.10.3. Conclusions Legal Aid Directive and relevance to the security industry .......... 78
3.5.11. Directive 2004/80/EC relating to compensation to crime victims ...................................... 79
  3.5.11.1. Brief summary of the regime .............................................................................................. 79
  3.5.11.2. Applicability in time ............................................................................................................ 79
  3.5.11.3. Conclusions Compensation Directive and relevance to the security industry ....... 79
3.5.12. Regulation 593/2008 on the law applicable to contractual obligations (Rome I) ........... 79
  3.5.12.1. Brief summary of the regime ............................................................................................ 79
3.5.12.2. Applicability in time ................................................................. 80
3.5.12.3. Conclusions Rome I Regulation and relevance to the security industry .......... 80
3.5.13. Regulation 864/2007 on the law applicable to non-contractual obligations
(Rome II) ............................................................................................ 81
3.5.13.1. Brief summary of the regime .................................................................. 81
3.5.13.2. Applicability in time ............................................................................. 82
3.5.13.3. Conclusions Rome II Regulation and relevance to the security industry ...... 82
3.6. Concluding observations .................................................................................. 82
3.6.1. Liability regimes .......................................................................................... 83
3.6.2. Regulatory regimes ...................................................................................... 83
3.6.3. Relevance for the security industry ............................................................. 84
3.6.4. Lessons for a future liability regime for the European security industry? .......... 86

Chapter 4 Analysis of comparable EU-Member States legislation and related case law ................................................................. 89

4.1. Introduction ....................................................................................................... 89
4.2. The Questionnaire ........................................................................................... 89
4.3. Comparison ....................................................................................................... 94
4.3.1. Bases of liability .......................................................................................... 94
4.3.1.1. Fault based liability ............................................................................... 94
4.3.1.2. Product liability .................................................................................... 98
4.3.1.3. Special liability regimes ......................................................................... 99
4.3.1.3.1 General instruments to tighten or increase liability regarding dangerous
activities ................................................................................................................ 99
4.3.1.3.2 Third party liability for airplanes, GMOs, nuclear installations, medical
products (pharmaceuticals) and environmental harm ........................................... 100
4.3.2. Relationship between tort liability and regulation ......................................... 106
4.3.2.1. Relationship between tort liability and regulation in general .................... 106
4.3.2.2. Specific regulations governing the risks of the security industry ............... 107
4.3.3. Causation ..................................................................................................... 107
4.3.3.1. Standard burden of proof regarding the burden of proof of causation .......... 107
4.3.3.2. Instruments to lighten the burden of proof regarding the proof of causation .... 108
4.3.4. Attribution of liability .................................................................................. 108
4.3.4.1. Multiple parties ...................................................................................... 108
4.3.4.2. Legal channelling of liability to one person .............................................. 109
4.3.5. Damages and available remedies................................................................. 109
4.3.5.1. Types of compensable damages ............................................................... 109
4.3.5.2. Exclusion of heads of damage by contractual agreement ............................ 111
4.3.5.3. Special instruments for mitigating the liability of the tortfeasor (liability caps,
reduction clauses) ......................................................................................... 111
4.3.6. Applicability in time (retrospective liability) .................................................. 112
4.3.7. Alternative compensation mechanisms ....................................................... 112
4.3.7.1. Alternative compensation schemes ......................................................... 112
4.3.7.2. Compensation schemes for victims of terrorism ....................................... 112
4.3.7.3. Special rules on case management ............................................................ 113
4.3.8. Suggested reforms in national literature ....................................................... 113
4.3.9. Successes and failures of the national approach ............................................. 114
4.4. The liability risks of the security industry ....................................................... 114
4.4.1. The liability risk of the security company towards the client ......................... 114
4.4.2. The liability risk of the security company towards third parties .................... 114
4.4.2.1. Direct claims of third parties against the security company ....................... 114
4.4.2.2. Recourse of the client against the security company and vice versa ............ 118
4.4.3. Liability of the security provider for damage caused by a natural disaster or
an act of terror ............................................................................................. 119
Chapter 5 Analysis of potential analogy bearing international law treaties on civil aviation, nuclear safety and environmental liability

5.1. Civil aviation ................................................................. 129
  5.1.1. 1952 Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (Rome Convention) ................................................. 129
    5.1.1.1. Brief summary of the regime .................................. 129
    5.1.1.2. Basis of liability .................................................... 129
    5.1.1.3. Liable persons (attribution of liability) ....................... 130
    5.1.1.4. Damage covered ..................................................... 130
    5.1.1.5. Exclusions and defences .......................................... 131
    5.1.1.6. Relationship with regulation ..................................... 131
    5.1.1.7. Financial security and compensation mechanisms ............ 132
    5.1.1.8. Rules of evidence .................................................. 132
    5.1.1.9. Conclusions Rome Convention and Relevance to the Security Industry ........ 132
  5.1.2. 1999 Convention for the Unification of Certain Rules for International Carriage by Air (Montreal Convention) ........................................ 132
    5.1.2.1. Brief summary of the regime .................................. 132
    5.1.2.2. Basis of liability .................................................... 133
    5.1.2.3. Liable persons (attribution of liability) ....................... 133
    5.1.2.4. Damage covered ..................................................... 133
    5.1.2.5. Exclusions and defences .......................................... 134
    5.1.2.6. Relationship with regulation ..................................... 134
    5.1.2.7. Financial security and compensation mechanisms ............ 135
    5.1.2.8. Rules of evidence .................................................. 135
    5.1.2.9. Conclusions Montreal Convention and relevance to the Security Industry .... 135
  5.2. Nuclear liability ............................................................ 135
    5.2.1. Origins and summary of the regimes ................................ 135
    5.2.1.1. Origins of the nuclear liability regime ......................... 135
    5.2.1.2. First generation nuclear liability conventions ................ 136
    5.2.1.3. Second generation nuclear liability conventions .............. 137
    5.2.1.4. Maritime nuclear liability conventions ........................ 138
    5.2.2. Basis of liability ..................................................... 139
    5.2.3. Liable persons .......................................................... 140
    5.2.4. Damage covered ........................................................ 141
    5.2.4.1. Limitation of liability ............................................ 141
    5.2.4.2. Damage covered ........................................................ 142
Chapter 6 Analysis of legal practices by industries exposed to analogous risks and by their insurers ................................................................................................................................................................................................. 181

6.1. Insurance: legal and economic background ........................................................................................................................................................................................................... 182
6.1.1. Insurance’s risk – reducing effects ........................................................................................................................................................................................................... 182
6.1.2. Insurance prerequisites ................................................................................................................................................................................................................. 183
6.1.3. First - and third-party insurance ........................................................................................................................................................................................................... 184
6.1.4. Conclusions Insurance Theory ....................................................................................................................................................................................................... 187
6.2. Industry practices within sectors exposed to analogous risks ........................................................................................................................................... 188
6.2.1. The software industry ......................................................................................................................................................................................................... 190
6.2.1.1. Nature of potential risk exposure .................................................................................................................................................................................................. 190
6.2.1.2. Current industry practices to limit exposure contractually ......................................................................................................................................................... 193
6.2.2. The pharmaceutical industry ................................................................................................................................................................................................... 197
6.2.2.1. Nature of potential risk exposure .................................................................................................................................................................................................. 197
6.2.2.2. Current industry practices to limit exposure ................................................................................................................................................................. 199
6.2.3. The meteorological industry ....................................................................................................................................................................................................... 201
6.2.3.1. Nature of potential risk exposure .................................................................................................................................................................................................. 201
6.2.3.2. Current industry practices to limit exposure ................................................................................................................................................................. 202
6.2.4. Relevance to the Security industry .................................................................................................................................................................................................... 204
6.2.4.1. Software industry ......................................................................................................................................................................................................... 205
6.2.4.2. Pharmaceutical industry ....................................................................................................................................................................................................... 207
6.2.4.3. Meteorological industry ....................................................................................................................................................................................................... 207
6.2.5. Conclusions Industry Practices in other sectors ................................................................................................................................................................. 208
6.3. Insurance of man-made disasters and terrorism ........................................................................................................................................................................................ 209
6.3.1. Man-made disasters: liability insurance .......................................................................................................................................................................................... 209
6.3.2. Supply side problems: the case for compulsory liability insurance ............................................................................................................................................. 210
6.3.3. Demand side problems ....................................................................................................................................................................................................... 211
6.3.4. Government support needed? ...................................................................................................................................................................................................... 211
6.3.4.1. The case for public-private partnerships .................................................................................................................................................................................... 212
6.3.4.2. Government providing an additional risk layer: nuclear and oil .................................................................................................................................................. 213
6.3.4.3. The Consorcio de Compensación de Seguros ................................................................................................................................................................. 214
6.3.4.4. The Fukushima case ............................................................................................................................................................................................................. 215
Chapter 7 The US SAFETY Act ................................................................. 239

7.1. Legal analysis of US SAFETY Act......................................................... 239
7.1.1. Background, rationale, and implementation ..................................... 240
7.1.2. Liability protections available under the SAFETY Act ..................... 241
7.1.3. Eligibility for SAFETY Act protections.................................................. 243
7.1.4. Criteria for granting SAFETY Act protection.............................................. 244
7.1.5. Forms and extent of protection available (Designation and Certification)...... 245
7.1.6. Insurance requirement and liability limit ................................................. 248
7.1.7. The application process and timeline ..................................................... 249
7.1.8. Assessment of effectiveness, and advantages and disadvantages .............. 250
7.2. US case law pertaining to third party liability compensation against security industry................................................................. 253
7.3. Assessment of the potential of the US SAFETY Act to shield European security industry against limitless third party liability ......................................................... 255
7.3.1. Geographic scope of application ............................................................. 256
7.3.2. Eligibility of EU-based companies............................................................ 256
7.4. Analysis of the differences between the US federal legal system and the necessary European Union supranational framework preconditions to conclude a similar legal act ................................................................. 257
7.4.1. EU powers and legislation regarding TPL of the security industry ............... 258
7.4.2. Institutional, procedural and substantive issues ........................................... 259
7.4.2.1. Institutional ............................................................................................. 259
7.4.2.2. Procedural .............................................................................................. 261
7.4.2.3. Substantive ............................................................................................ 261

Chapter 8 Conclusions and policy options .................................................... 263

8.1. Separate treatment of the security industry? ............................................. 264
8.1.1. Liability exposure of the European security industry de lege lata .................. 265
8.1.2. Comparison with the US ........................................................................... 269
8.1.2.1. The liability litigation environment in the US and Europe .................... 269
8.1.2.1.1 Introduction ......................................................................................... 269
8.1.2.1.2 Summary of differences between US and European liability litigation ..... 269
8.1.2.1.3 Procedural aspects of the US system ..................................................... 271
List of References .............................................................................................................. 335

Annex I: Common format for analysis .............................................................................. 355

Annex II: Overview of stakeholder participants ............................................................... 359

Annex III: Country reports (in separate file) ................................................................. 333
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCR</td>
<td>Caisse Centrale de Réassurance</td>
</tr>
<tr>
<td>CCS</td>
<td>Consorcio de Compensación de Seguros</td>
</tr>
<tr>
<td>CFR</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>CLC</td>
<td>International Convention on Civil Liability for Oil Pollution Damage</td>
</tr>
<tr>
<td>CLP</td>
<td>Classification, Labelling and Packaging</td>
</tr>
<tr>
<td>CMR</td>
<td>Carcinogenic, Mutagenic of Toxic to Reproduction Substances</td>
</tr>
<tr>
<td>CPR</td>
<td>Construction Products Regulation</td>
</tr>
<tr>
<td>CRISTAL</td>
<td>Contract Regarding an Interim Supplement to Tanker Liability for Oil Pollution</td>
</tr>
<tr>
<td>CSC</td>
<td>Convention on Supplementary Compensation</td>
</tr>
<tr>
<td>ECHA</td>
<td>European Chemicals Agency</td>
</tr>
<tr>
<td>EEELR</td>
<td>European Energy and Environmental Law Review</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention for the Protection of Human Rights and Fundamental Freedoms</td>
</tr>
<tr>
<td>ELD</td>
<td>Environmental Liability Directive</td>
</tr>
<tr>
<td>GAREAT</td>
<td>Gestion de l’Assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme</td>
</tr>
<tr>
<td>GMO</td>
<td>Genetically Modified Organism</td>
</tr>
<tr>
<td>GPSD</td>
<td>General Product Safety Directive</td>
</tr>
<tr>
<td>HNS</td>
<td>Hazardous and Noxious Substances by Sea</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organisation</td>
</tr>
<tr>
<td>IPPC</td>
<td>Integrated Pollution Prevention and Control</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>NHT</td>
<td>Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden</td>
</tr>
<tr>
<td>OJ</td>
<td>Official Journal</td>
</tr>
<tr>
<td>PLD</td>
<td>Product Liability Directive</td>
</tr>
<tr>
<td>PPE</td>
<td>Personal Protective Equipment</td>
</tr>
<tr>
<td>PPPR</td>
<td>Plant Protection Product Regulation</td>
</tr>
<tr>
<td>REACH</td>
<td>Registration, Evaluation, Authorisation and Restriction of Chemicals</td>
</tr>
<tr>
<td>RPP</td>
<td>Regulation Payment Procedure</td>
</tr>
<tr>
<td>SDR</td>
<td>Special Drawing Right</td>
</tr>
<tr>
<td>SI</td>
<td>Security Industry</td>
</tr>
<tr>
<td>SL</td>
<td>Strict Liability</td>
</tr>
<tr>
<td>TEPCO</td>
<td>Tokyo Electric Power Company</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>TOVALOP</td>
<td>Tanker Owners Voluntary Agreement concerning Liability for Oil Pollution</td>
</tr>
<tr>
<td>TPL</td>
<td>Third Party Liability</td>
</tr>
<tr>
<td>TRIA</td>
<td>Terrorism Risk Insurance Act (US)</td>
</tr>
</tbody>
</table>
Executive Summary

1. Introduction and background

Third party liability has been identified as an issue that could adversely impact the European security industry. Limitless third party liability for security product and services is believed to have the potential to reduce investments in innovation. In the US, the Safety Act (which is further discussed in Section 3, below) has been enacted to empower the government to provide protection against liability exposure. This development has convinced the EU to examine the legal implications of third party liability of the security industry and possible policy options. To this end, the Commission, DG ENTR, has commissioned this study, which has been carried out by METRO (University of Maastricht), ECTIL, and Hunton & Williams.

The main objectives of this study are:

- To collect, analyze and assess data from various legal sources and actual best practices related to the field of third party liability;
- To provide a comprehensive overview on the current status of third party liability-related legal implications for security industry,
- To provide a portfolio of feasible policy options for the Commission to address these implications effectively, taking into account that the findings and their respective reasoning will present the potential basis for wide ranging policy decisions by the European Commission.

Thus, this study focuses on understanding the third party liability exposure of the EU-based Security Industry (SI), analyzes the US Safety Act and its context, and identifies policy options relating to the SI’s liability exposure.

2. Definition of security industry and methodology

There currently is no clear, generally accepted definition of the security industry; this sector of industry, for instance, is not covered as such by the main statistical nomenclatures. Any specific initiative or measure for the security industry, of course, would require a clear and unambiguous definition.

The security industry includes a potentially very broad scope of activities. The market for security goods and services has three distinctive features: (1) it is a highly fragmented market and divided along national or even regional boundaries; (2) it is an institutional market, and buyers tend to be public and semi-public authorities, and (3) this market has a strong societal dimension, as personal safety is regarded as a highly sensitive area.

For purposes of guiding the research and analysis required for this study, based on literature, market research, and Commission documents, a pragmatic, objective and comprehensive definition of the security industry was developed. It is recognized that the security industry provides products (e.g. detection equipment, alarm systems) and services (e.g. guarding services), and addresses man-made and natural risks; this study, however, covers only man-made risks.

The Commission Action Plan for innovative and competitive Security Industry lists the following: aviation security; maritime security; border security; critical infrastructure protection; counter-terror intelligence (including cyber security and communication); crisis management/civil protection; physical security protection; and protective clothing. For this
study, only the industry producing goods and services used for mitigating damages by terrorism and organized crime is considered ‘security industry.’

Thus, the security industry has been defined to include ‘providers of products and services that are specifically intended to reduce the risks of intentional damage caused by terrorism and organized crime in the following areas: aviation security, maritime security, border security, critical infrastructure protection, and physical security protection.

- The following products and services are regarded as being provided by the security industry: scanning and detection equipment for use with passengers and cargo (or other goods), including products for weapons and explosives detection, chemical and biological risk detection, and radionuclide detection, as well as services related to all of the above.

- The following industries are NOT part of the security industry for the purposes of this study: defense industry, building monitoring and management industry, plant automation and control industry, scientific automation industry, ICT industry, software, information technologies, other providers of products and services that are not specifically intended to reduce the risks of intentional damage caused by terrorism and organized crime, such as providers of fences, reinforced glass, etc.

Note, however, that the study team used this definition only to guide its thinking. The research and analysis conducted has gone beyond the scope of the definition.

In conducting the research and analysis required for this study, three methodological approaches have been followed: (1) legal analysis, including desk research and comparative legal analysis; (2) economic analysis of law, including analysis of the effects of liability on operators exposed to it, insurance-related aspects, and benefits and costs of options and alternatives; and (3) empirical research, where necessary, focusing on actual practices of operators and insurers, and involving semi-structured interviews with stakeholders on the basis of questionnaires. To guarantee comparability of results, we used checklist to analyze various liability regimes.

3. Analysis of comparable EU legislation and related case law and potential analogy-bearing international law treaties

As part of the study, a series of EU legislative and other instruments and international liability treaties have been analyzed. The liability regimes laid down in these instruments have been analyzed with respect to the following key features: (i) basis of liability, (ii) relationship with regulation, (iii) causation, (iv) attribution of liability, (v) damages/remedies, (vi) applicability in time, (vii) compensation mechanisms, and (viii) jurisdictional issues.

The analysis of the regulatory regimes included in the study focused on the relationship between regulation and liability law, and on how non-compliance with regulation can increase liability exposure, and how compliance can limit liability exposure.

This analysis focused on the relevance of the instruments concerned for the security industry. The first question was whether the regimes cover or can be applied to security providers. The second question was to what extent the instruments analyzed provide interesting lessons for a possible future liability regime for the security industry.
4. Analysis of comparable EU-Member States legislation and related case law

The TPL exposure of SI providers is a function of national law, not EU law. EU law is only indirectly relevant, e.g. the Product Liability Directive shapes the national product liability regimes.

The analysis of the national laws of seven EU Member States (England, France, Germany, Netherlands, Poland, Spain, and Sweden) and related case law lead to the following conclusions:

- There is no special case law with respect to the third party liability of security companies in the analysed jurisdictions, with a few exceptions.

- The liability of the security provider towards the client is regulated by the contract. The contractual freedom is only limited by rules concerning the fairness of contractual clauses. The contract is also essential for the recourse obligation of the security provider towards the client.

- Liability for the secured activity towards third parties lies primarily with the client who is liable under fault based liability or under various, rather inconsistent national rules on strict liability. Recourse of the client against the security provider is only possible, if the security provider himself is liable towards the third party (recourse under joint and several liability) or if recourse is provided by the contract.

- Only if the security provider contractually agrees with the client to take over the whole responsibility to provide for the security of an activity or facility, he will assume an independent duty in torts to protect third parties from harm caused by this activity or facility (theory of the liability of the independent contractor). This liability is fault based and will not cover pure economic loss.

- The security provider is not under an obligation of strict liability under national law. Applicable liability regimes are only fault-based liability or, for the producer of a security device, product liability.

- Fault based liability requires that the security provider breached a duty of care. These duties are defined by the contract with the client. The security provider cannot be held liable by the client or any third party for the fact that the stipulated measure, device or security standard does not meet the highest standard provided by the industry. Liability can in this case only arise if the security provider who knew or should have known that the security measures are inadequate failed to inform the client of this fact.

- Fault based liability covers in all jurisdictions damages for personal injury, harm to property and consequential economic loss. Compensation for pure economic loss and for environmental damage is rather restricted.

- Liability under product liability is determined by the EU-product liability directive. Liability encompasses manufacturing, design and warning (marketing) defects. The product must meet an objective safety standard (according to technical standards etc.) which, however can, according to Article 6 (1) (a), be specified inter alia by the presentation of the product by the producer (e.g. sales promotion, sales contract, instructions for installation and use). The producer of a security device will thus not be liable for the mere fact that another product on the market would have achieved a higher security standard. The exposure under European product liability law is limited...
to personal injury and property damage to private persons, excluding pure economic loss and punitive damage.

- If harm is caused by a natural disaster or by an intentional act of a third person, the security provider will only be liable if he had a duty of care to prevent the occurrence of such damage. With respect to the client, the duty of care of the security provider will be specified by the contract. With respect to liability towards third persons, the question whether the security provider owes them a duty of care or not must be assessed according to general tort law. For this assessment the contractual obligations of the security provider towards the client are very important. Liability can only be imputed to the security provider if his contractual duties implied the prevention of such damage. Even when the security provider assumed responsibility for the prevention of such damage in the contract he may not be directly liable to third parties as the link between the carelessness of the security provider and the sustained damage may be assessed to be too remote to trigger liability.

- Under strict liability such events (natural disaster, terrorist attack) are in most countries qualified as ‘force majeure’ or ‘act of god’ and may exonerate the person who is subject to the strict liability regime from liability. This defence applies only to the client and not to the security provider, who is only under an obligation of fault based liability. For the security provider it is of indirect relevance, as there will be no recourse obligation towards the client, if the client is not liable.

- Damage caused by terrorist attacks is often compensated by the state. In France, Spain and the UK special compensation schemes for victims of terrorism are established. While the British compensation only grants compensation to victims of terrorism who cannot obtain compensation from other sources, the French and the Spanish compensation scheme provides for subrogation.

- All of the analysed national legal systems provide for special rules on case management, but none of the analysed national legal systems provides for a US-style class action.

5. Analysis of the US Safety Act and liability system

The US Safety Act was enacted after 9/11 litigation mushroomed. Court cases were filed against several categories of defendants, including SI providers. The US legislature responded to these developments by providing for a regime of TPL protection.

The US legislature’s concern was that in a litigious environment security companies would not innovate and not make new products available out of fear of claims. To alleviate such fears, the US Safety Act authorizes case-by-case limitation of a security provider’s liability exposure, subject to an obligation to contract insurance coverage up to a limit specific in an individual case. If protection under the Act is granted, punitive damages are excluded and suits can be brought only before Federal courts. Both US and non-US security providers can apply for protection under the Safety Act.

The protection granted pursuant to the Safety Act is not effective in the EU. This is true for US and non-US, including EU, companies. Accordingly, this protection does not directly affect competition in the EU; it may indirectly provide an advantage to US-based companies where it creates a favorable environment for the development of innovative security products and services.
The rationale for the US Safety Act is closely related to the litigation environment in the US, which is very different from the EU situation. Important differences include the phenomenon of ‘discovery’ in US litigation (which is not part of the European system), the use of experts (so-called ‘hired guns’), decision-making by juries (as opposed to professional judges), and contingency fees (which are an almost exclusively US phenomenon). Further, awards for pain and suffering can be very substantial in the US, and punitive and treble damages exist only in the US, not in the EU (with the exception of English law, which does provide for punitive damages, but not in relation to damages that might affect the Security Industry).

6. **Policy options**

The EU Treaties and laws do not prevent the adoption by the EU of measures limiting TPL of SI providers, as long as the Treaty is respected. The EU is competent to adopt such rules based on its internal market powers, but any such measures are subject to the subsidiarity and proportionality principles. This means that any measures should be proportional to the problem to be solved.

In this case, potential TPL exposure of EU SI providers is not (yet) an actual problem in practice. Although financial limits are not in place, liability of security providers for terrorism-related damage requires proof of negligence and such liability can be limited by contract. Further, the liability standards and litigation environment in the EU do not encourage unmeritorious claims and, consequently, the SI’s potential liability exposure is limited. EU legislation on TPL exposure of SI providers therefore is not indicated.

Having noted this, SI providers may be uniquely exposed to potential TPL due to a combination of four factors: (i) there is potential exposure to unlimited catastrophic liability; (ii) they provide security, typically deemed (and closely related to) a government responsibility; (iii) they report experiencing difficulties in obtaining adequate insurance coverage at affordable premiums; and (iv) they claim that they cannot limit their liability by contract, in particular with public authorities in procurement procedures. These factors, however, should be understood in the context of the facts and applicable laws, and do not in themselves justify a liability limitation.

An important consideration for policy makers is that liability exposure creates incentives for prevention and limiting liability may thus reduce such incentives. Liability also plays a role in allocating risks and spreading losses. Where the law imposes liability for damage that is beyond the liable party’s control, however, it may become counter-productive, but the study found no evidence of such excessive liability exposure.

Further, any measures to limit the TPL of SI providers raises the question of who will compensate the damage that may arise: other economic operators or the government? The rationale for having other parties or the government pay compensation is weak in cases where the SI provider involved was in the best position to prevent the damage. A TPL limitation only for SI providers also raises the question why only they should receive this benefit.

Subject to these considerations, possible options to address TPL of SI providers include the following:

- An EU Safety Act modeled along the lines of the US Act: The case for such an act is weak given the lack of actual cases and the much more balanced EU litigation environment.

- Direct, generally applicable liability limitations for the benefit of SI providers, such as (i) financial caps and limits, (ii) exclusion of certain heads of damage (e.g., pure
economic losses); (iii) channeling of liability (liability imposed exclusively on one party, e.g. operators of facilities); (iv) causation-related restrictions (e.g. only direct damage); (v) regulation-related restrictions (e.g., a regulatory compliance defense). The need and justification for such limitations are not clear, however, and possible adverse effects should be considered.

- Procedural devices, such as (i) litigation management (centralization of simultaneous law suits; multiple laws may apply, however), and (ii) exclusive jurisdiction rules (e.g. for member state in which incident occurred). Such measures, by their nature, do not affect substantive rights to compensation of damages suffered, but they would deprive Member State courts of jurisdiction.

- Victim compensation solutions (e.g., funds, government-provided compensation, government assumption of excessive risk, mandatory financial security). Any such measures will raise questions such as who must contribute to fund and on what basis. The adverse effects on incentives is possibly an issue, in particular with government funding or significant cross-subsidies. On the other hand, government assumption of excessive risk could stimulate the insurance market, if necessary.

- Mandatory financial security may help to address potential insolvency, but is inefficient unless there is a a competitive insurance market. Again, the need and justification are weak at best.

- Initiatives addressing issues in market for security goods and services, e.g. in contracting for liability limitations. To the extent this market does not function well in allocating liability risks (i.e., no liability limitations are granted by (semi-)public entities), a limited, specific initiative could analyze and help to resolve this problem; the security and insurance industry should play a key role here.

- Initiatives aimed at the insurance market, e.g. to facilitate offering of adequate policies at competitive prices (with or without the government assuming a layer of excessive risk). To the extent the insurance market does not offer adequate coverage at reasonable prices (which security providers should first demonstrate), a limited, specific initiative to stimulate coverage could be considered.

- Initiatives aimed at educating stakeholders and facilitating the exchange of information to prevent issues in the future. Given the current confusion among security industry stakeholders over key issues such as the nature and scope of liability exposure, such initiatives are easily justifiable.

With respect to form, EU measures or initiatives could involve binding legislation, non-binding policy initiatives, or facilitating initiatives. For instance, a Commission recommendation similar to the Commission Recommendation on auditors’ liability would be a non-binding initiative. An alternative would be a Commission communication. Such a recommendation or communication could build on some of the trends identified in this study, such as that SI providers are not responsible for the choice of security goods and services, and should not be held liable merely on the basis of an incorrect choice.

7. Conclusions

This study has not found any evidence of an impending liability crisis in the security industry. The assertions of ‘enterprise-threatening’ liability exposure are not consistent with the liability standards imposed by the laws of the Member States covered in this study. No urgent
EU measures are therefore necessary. To prevent problems in future cases, a Commission recommendation or communication could be considered.

Security industry representatives have also claimed that there are problems in the insurance market and in the market for public procurement of security goods and services. The industry could be invited to provide further evidence and analysis of any such issues.
Chapter 1 Introduction

1.1. Background

1.1.1. Increasing exposure to risks...

The background for the project is nicely sketched in the Invitation to Tender. The German sociologist Ulrich Beck has eloquently explained in his book *The Risk Society* that as a result of the technological revolution, citizens are increasingly exposed to a variety of risks that to some extent are precisely related to new technologies. Human actions therefore seem to have increased the number of risks that society is exposed to. The Invitation to Tender already mentions the terrorist attack on 9/11 and the Deepwater Horizon incident in the Gulf of Mexico. In addition to this (seemingly increasing) exposure to technological risks (also referred to as man-made disasters) the number of natural disasters is also increasing. Reinsurers claim that the insured losses due to natural catastrophes increased substantially in the period 1970-2007, whereas the insured losses resulting from man-made disasters seemed to remain constant.¹ However, increasingly the distinction between man-made and natural disasters becomes blurred. A striking example constitutes hurricane Katrina. Whereas the hurricane itself is undoubtedly a natural disaster, the massive impact of Katrina is, according to many, largely due to failure of public authorities, both in the precaution towards Katrina but also in providing relief.² Also: the nuclear incident at the Fukushima power plant was undoubtedly triggered by a natural event (the tsunami), but questions can be asked both concerning the location of the power plant in an earthquake zone³ as with respect to the location of the reserve diesel generators for the cooling system in an area which was vulnerable to flooding. Also, climate change and the depletion of the ozone layer are indicated as examples where human activities can trigger catastrophic “natural” disasters.⁴

1.1.2. … leads to a new security industry

These (and many other) examples illustrate the increasing exposure of society (including obviously Europe) to many risks, some of which can bring disaster. This has created an industry which is active in various ways in preventing the (impact of) disasters. Technological development is of course key to preventing disasters of all kind. The industry involved in the prevention of the (impact of) disasters is referred to as the security industry.

Differently than in the US, the security industry in Europe is still widely unregulated. The unregulated character of industry may at first blush have the advantage that it creates a wide scope for the industry to develop; the disadvantage is that a lack of regulation could lead to a potentially unlimited liability. The danger of a lack of regulation may hence lead to an inability of undertaking socially beneficial activities (more particularly developing new technologies aiming at increased security) out of fear for liability. From that perspective, a lack of regulation is not necessarily a benefit for society but may lead to the perverse result that socially beneficial investments are not taking place out of fear for an unlimited liability.

In this respect, an interesting parallel can be made e.g. with the development of nuclear energy: when nuclear power developed in the 1950s, there was on the one hand a strong belief

---

¹ See Kunreuther 2008, p. 5.
³ For a critical analysis see Ramseyer 2011.
⁴ For a further analysis see Viscusi and Zeckhauser 2012.
in the potentially desirable effects of this new energy source, but at the same time especially suppliers of nuclear material (at that time exclusively US based) feared potentially limitless liability which could inhibit the further development of investments into nuclear energy. That is why two studies were initiated at the end of the 1950s analysing how an appropriate liability regime could encourage the development of the nuclear sector.\(^5\) The result was the creation of the international legal framework for nuclear liability consisting \textit{inter alia} of the conventions of Brussels and Paris (drafted within the framework of the nuclear energy agency of the OECD) on the one hand and of Vienna (drafted in the framework of the international atomic energy agency) on the other. These conventions \textit{inter alia} created strict liability and introduced compulsory insurance, but at the same time channelled liability exclusively to the operator of a nuclear plant, thus limiting liability exposure of potentially other involved parties and put a financial cap on the liability of the operator. In addition, a second and third layer of compensation was provided by the installation state (second layer) and all participating states in the convention (third layer).

1.1.3. Need for a clear liability regime

To some extent one could compare the security industry in the EU today with the nuclear industry in the 1950s. On the one hand, society demands a development of this type of industry, but on the other hand, a lack of regulation of the liability regime (or at least a lack of sufficient clarification and certainty) may inhibit efficient investments in research and development.

A complicating factor (which also played in the development of nuclear liability in the 1950s) is that uncertainty concerning the potential scope of liability may endanger the insurability of the risks. Traditionally, predictability of risks is one of the cornerstones to make liability risks insurable.\(^6\) Factual and legal uncertainty may endanger this insurability.\(^7\) Hence, the current uncertainty concerning the scope of liability of the EU security industry may endanger the insurability of the risk. Again, the lack of financial coverage (via insurance or alternative compensation mechanisms) may lead risk-averse operators to refrain from efficient investments in research and development in the EU security industry. From an insurability perspective a clarification of the scope of liability of the EU security industry is important if one wishes, as a policy goal, to promote the development of this security industry. Given society’s increasing exposure to risks, evidently also in the EU, the desirability of the development of such a security industry can hardly be debated. Hence, the background for this study is to find an appropriate scope for the liability of the EU security industry.

1.2. Goals

The goals of the study are clearly stated in the Invitation to Tender and will therefore be the leading goals for this study:

- To collect, analyse and assess data from various legal sources and actual best practices related to the field of third party liability;
- To provide a comprehensive overview of the current status of third party liability related legal implications for the security industry as well as an overview of policy options for the European Commission;

\(^5\) The so-called Preliminary Report and the Harvard Report. For details see Van den Borre 2007, p. 263-266.
\(^6\) See Faure and Hartlief 2003, p. 84-85.
\(^7\) See Monti 2001, p. 51-79.
To present the potential basis for wide-reaching policy decisions by the European Commission, understandable by both laymen as well as legal experts.

1.3. A few starting points

In order to tackle this highly interesting but broad topic we will follow a few general starting points:

- First, we will pay attention to potential goals of a liability system. Identifying those goals (e.g. deterrence, compensation or insurability) may be crucial since they can lead the final policy recommendations.
- Second, following these goals, we propose to pay attention to a normative framework, largely based on a law and economics methodology, that will enable us to indicate the desirability of a particular liability regime. Without a normative framework one would merely analyse a variety of different legal regimes without knowing precisely why one regime of third party liability would necessarily be better than another. Therefore, developing such a normative framework is indispensable if best practices should be developed concerning the field of third party liability.
- Third, this normative framework will include a checklist with criteria for liability which will enable us to judge whether a particular liability regime that we will analyse has to be assessed as reasonable, effective or rather crushing and inefficient. The checklist with these criteria will be further explained in the methodology below.
- Fourth, we will use this checklist with criteria for judging liability to analyse the existing third party liability regimes mentioned in the work packages. Again, the advantage of this approach is that the way in which the third party liability regimes to be addressed in the various work packages will be analysed shows some degree of harmonization and hence comparability.
- Fifth, the analysis of the various third party liability regimes will lead to recommendations concerning various policy options for EU action.
- Sixth, the different liability systems that will be analysed in detail in the various work packages will hence be studied within this project from two angles: first, the question will be asked to what extent the regimes studied (e.g. concerning product liability or REACH) could be applicable to services or products provided by the safety industry. Second, the liability regimes will be analysed to ask the question to what extent they can constitute an interesting example or contain an interesting feature for a possible EU regime concerning the liability of the security industry.

1.4. Methodology

In this study basically three methodological approaches will be followed. Moreover, in order to guarantee the comparability of the results, we have developed a checklist that can be used to analyse the various liability regimes that will be discussed in the different chapters.

1.4.1. Three methodological approaches

The following methodological approaches will be used in this project:

1.4.1.1. Legal analysis

The legal analysis will in turn consist of two approaches. The first and obvious one is legal desk research. This research requires a detailed analysis of primary legal sources providing
information on the goals and working of the particular legal regimes identified in the work packages. For every liability issue to be addressed in the work packages a detailed literature study will be conducted. Many of the legal rules to be analysed originate from European rules or international conventions and therefore a vertical comparative legal approach is necessary to analyse the implementation in national law of Member States. This will be followed by a horizontal comparative legal approach addressing differences between the Member States. The way in which these liability regimes identified in the work packages will be analysed is again on the basis of the checklist described.

A comparison of the legal systems of EU Member States seems necessary, as (despite many similarities in most areas) there are important differences and very often no common core among the respective national legal systems. If the EU aims at harmonization or unification of law, it has to try to draw up a consistent concept which is acceptable to all or at least to most of the Member States. Otherwise the Member States will not agree to harmonize the area of law under discussion. Further, if directives are at stake which cover only small areas, the danger is that these directives will neither accord with other directives nor fit in the national legal systems and therefore result in increased inconsistency. Last but not least, one is inspired by studying foreign legal systems, by trying to understand other ways of legal thinking, by discovering new tools for solving problems, and by hearing about different experiences and solutions in other countries.

Hypothetically, one could also look at e.g. the liability of a Member State. However, state liability is excluded from the analysis in this report, except to the extent that it is relevant to the Security Industry’s liability.

1.4.1.2. Law and economics

The second approach to be followed, in addition to the more traditional legal (comparative) approach, is a law and economics methodology. The law and economics methodology provides insights on the working of liability rules and the effect of particular elements of the liability rules on the stakeholders involved, more particularly the operators exposed to liability. Hence, law and economics is extremely useful to address the crucial issue of this project; being how the various aspects of a liability regime affect the scope of liability of the operator in the security industry.

An important part of law and economics, especially the economic analysis of accident law,8 addressed the scope of liability in the light of the insurability of a liability regime. Precisely because the insurability of liability may be crucial for operators active in the security industry, this insurability aspect will be taken into account when addressing the scope of liability.

Law and economics furthermore has the advantage of not only pointing at the potential dangers created by particular activities, but also at their benefits, the so-called positive externalities for society. These may play an important role in case of the safety industry. The positive externalities created by the safety industry may provide a reason to limit liability, which is a crucial aspect of this project.9

---

8 As it has been strongly developed inter alia by Shavell 1987.
9 See Gilead 1997, p. 589.
1.4.1.3. **Empirics**

An analysis into actual best practices can obviously not only be done by means of desk research. Some of the questions in particular work packages, for example concerning the practice of insurers towards large-scale natural disasters, therefore also require field research analysing how insurers work in practice and what type of coverage is provided. This is the case for many other questions within the various work packages as well.

Hence, to the extent that a work package requires this, also an empirical approach will be followed. Usually this will consist of semi-structured interviews. These will be prepared on the basis of a questionnaire, after which interviews will be held with selected stakeholders, who are experts in the particular domains.

1.4.2. **Checklist**

In order to be able to compare the results, especially when analysing the liability and regulatory regimes, we developed a common format which could be considered as a checklist for analysing liability regimes and for regulatory programmes. Different formats have been developed for analysing liability regimes and regulatory regimes, respectively. These formats will be applied in the legal analysis, the result of which can mainly be found in Chapters 3, 4 and 5.

In addition to using a common format for the analysis of the liability or regulatory regime concerned we have also always examined to what extent the regime examined affects the liability exposure of security services providers. In addition we have analysed whether any of the concepts or features of the regime we studied could be usefully applied in determining the potential liability regime for the security industry. Therefore, as we indicated above, the legal analysis always had this double focus by on the one hand focusing on the applicability of particular regimes to the security industry and on the other hand examining, more in an abstract manner, to what extent particular regimes could constitute an interesting example for the security industry.

1.5. **Structure**

After this introduction, the various chapters will largely follow the work packages identified in the Invitation to Tender and our technical offer. However, before starting the analysis we found that a crucial issue throughout this study is of course how one can define the security industry. Security services or products can potentially include a wide variety of different aspects. We considered it important at the outset of the study to provide a few indications of how one could define the security industry. We also provide a justification for the way in which we will ourselves interpret the security industry within the scope of this study. It is important to do this at the outset, since it obviously has an important influence on the scope of potential liabilities or future liability regimes. Therefore Chapter 2 starts with an attempt to define the security industry. Chapter 3 provides an analysis of comparable EU legislation and related case law. Subsequently, Chapter 4 provides an analysis of comparable EU Member States legislation and related case law. In Chapter 5 we will then present an analysis of potential analogy bearing international law treaties on civil aviation, nuclear safety and

---

10 This corresponds to Work Package 1 of the Invitation to Tender.
11 This corresponds to Work Package 2 of the Invitation to Tender.
environmental liability. Chapter 6 provides an analysis of legal practices by industries exposed to analogous risks towards third party liability risk limitations. Chapter 7 includes a legal analysis of the US Safety Act. Finally, Chapter 8 provides a formulation of legal and technical options for implementing a feasible third party liability regime in the EU.

At the end of this report we include a list of literature references for all chapters. The study concludes with a list of annexes, among which the common format for analysis of liability and regulatory regimes to which we referred above (Annex I). Another important annex is an overview of stakeholders with whom we had contacts within the framework of the execution of the empirical approach (Annex II).

---

12 This corresponds to Work Package 3 of the Invitation to Tender.
13 This corresponds to Work Package 4 of the Invitation to Tender.
14 This corresponds to Work Package 5 of the Invitation to Tender.
15 See 1.4.1.3 above.
Chapter 2 A definition of the security industry in Europe

2.1. Introduction

The security industry encompasses potentially a very broad scope of activities. Although it does not seem appropriate to narrow down the definition of security industry too much since the scope of the project should not ab initio be limited, it may be appropriate in an early phase of the project to define how the notion of security industry should be interpreted for the purposes of this report.

Indeed, one of the questions that may arise is whether one will focus only on industrial activities aiming at the precaution of particular risks or also at activities aiming at the mitigation of damages, which could include relief activities after a disaster. Also, the scope of (catastrophic) risks that the security industry could prevent can diverge widely from natural disasters (like flooding) to terrorism risks, cyber crime and technological disasters. The branches of industry involved in preventing risks in those different areas may largely vary.

2.2. A definition of the security industry in Europe

The global security market is estimated to be worth some €100 billion with around 2 million persons employed worldwide. The EU security market has an estimated market value in the range of €26 billion to €36.5 billion with around 180,000 employees.\(^\text{16}\)

However, there is currently no clear definition of the security industry. A methodical classification of this industry is hindered by a number of factors:\(^\text{17}\)

- The security industry is not covered as such by the main statistical nomenclatures (NACE, Prodcom, etc.).
- The production of security-related items is hidden under a wide range of headings. Statistics for these headings do not distinguish between security and non-security related activities.
- There is no statistical data source available at European level from the industry itself.
- From a supply-side perspective, procurers of security equipment and systems can be reluctant to provide information on security expenditures.

Moreover, the security market has three distinctive features, which distinguishes it from other industries:\(^\text{18}\)

(1) It is a highly fragmented market divided along national or even regional boundaries. Security, being a very sensitive policy field, is one of the areas where Member States are hesitant to give up their national prerogatives.

---


(2) It is an institutional market. The buyers of security services mostly are public authorities. And even in areas where it is a commercial market, the security requirements are still largely framed through legislation.

(3) It has a strong societal dimension. Although security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies may have an impact on fundamental rights and might provoke fear of a possible undermining of privacy.

Research was carried out on the available literature to find a common and widely accepted definition of the security sector. A starting point might be the definition of Carlos Marti Sempere\(^{19}\) which states:

The security industry is understood as the industry that supplies the products and services specifically used by the human being to identify, prepare, prevent, protect, respond, reduce, palliate and deal with the threats and consequences that undesired events have on society. These consequences may be summarized in terms of damage to people’s life, health, property or other assets, including information.

This definition can be used to further develop a pragmatic, objective and comprehensive definition of the industry for the purposes of this report.

### 2.3. A conceptual definition of the security industry

A possible way to limit the definition of the security industry is to look at the perceived security risks by European citizens and stakeholders, and at the tasks that have to be fulfilled in order to deal with these security risks. From these facts, industry that belongs to the security industry and industry that must be considered outside the security industry can be defined and visualized.

The remainder of this chapter is structured as follows: first, the security challenges perceived by stakeholders/EU citizens will be addressed. Next, the main tasks of the security industry will be examined. This information will serve as a basis to examine who is the security industry. Concluding, the main findings will be summarized in a conceptual scheme of the security industry.

### 2.4. What are the security challenges perceived by stakeholders/ EU citizens?

First, the five security missions on which EU stakeholders are focusing are protection against terrorism and organized crime, border security, critical infrastructure protection, and restoring security in case of crisis. These missions require a comprehensive suite of internal and external security instruments covering intelligence, police, judicial, economic and technological means.\(^{20}\)

With respect to EU citizens, the Eurobarometer Survey on Internal Security, published on 25 November 2011 accompanies the first annual report on the implementation of the EU Internal Security Strategy (ISS) (IP/11/1453).\(^{21}\) The main results of the Survey are:

- The main challenges to European security, identified by at least one in five Europeans, are the economic and financial crises (34%), terrorism (33%), and organised crime (21%).

\(^{19}\) Martí Sempere 2010, p. 4.

\(^{20}\) See esd-partners.com.

Poverty, irregular immigration, corruption, environmental issues/climate change, natural and nuclear disasters and the security of EU borders were also cited by around 18% of respondents. Fewer than one tenth of Europeans mentioned wars and civil wars, religious extremism, and petty crime as the most important security challenges faced by the EU (see table 1 below).

- The main challenges to national security, as identified by at least one in five Europeans, are the economic and financial crises (33%), terrorism (25%), poverty (24%), and organised crime (22%). Some 18% also mentioned corruption, irregular immigration, petty crime, natural disasters, environmental issues/climate change and cybercrime. Fewer than one tenth of respondents mentioned nuclear disasters, the security of EU borders, religious extremism, and wars and civil wars as the most important security challenges faced by their country (see table 2).

- Cybercrime is seen as the challenge most likely to heighten over the next three years (63%). This is followed by organised crime (57%), and then disasters (54%) and terrorism (51%). One in four respondents (43%) thinks that EU border security will be an increasing challenge to EU security over the next three years.

- Three-quarters of Europeans believe that internal EU security is linked to external events and developments, although there is considerable variation between Member States. The US is the most often cited as the EU’s main partner in security, followed by Russia, China and Turkey.

The following tables illustrate the above findings graphically.

---

Table 1: Eurobarometer 371, “Internal security”, European Commission, November 2011
Based on the main findings of the Survey, there are 5 main sources of insecurity as perceived by EU citizens:

Five main sources of insecurity:
- Terrorism
- Organised Crime
- Cybercrime
- Border Security
- Natural and Nuclear disasters

Despite the fact that the economic and financial crisis is mentioned by the European citizens as the main challenge to security, this feeling of insecurity might be more related to economic losses and unemployment, rather than real security risks as such. Therefore, the economic and financial crisis is not mentioned in the five main sources of insecurity.

Furthermore, for the purpose of the current study, it might be necessary not to focus on all 5 sources of insecurity but to target the most important insecurity risks.

Next, it merits to examine which types of activities or which tasks the security industry performs, again with the idea to define the scope of the European security industry.
2.5. Main tasks of the security industry

There is a plethora of policies and instruments to abate terrorism and organized crime. In order to get an overview and to be able to delimit the security industry, we can group the main tasks of the security industry as follows:\textsuperscript{22}

- \textit{Intelligence and surveillance}. This is an essential task. It involves technologies to: (a) gather information of people, assets and behaviours; (b) monitor sites and areas; (c) detect concealed weapons and operations’ plans, and (d) maintain the profiles, databases and systems to exploit such information once collected. The knowledge gathered can be used to disrupt terrorists’ operational and logistic chain, cutting off their access to money, weapons, knowledge, technologies, infrastructures, and other resources; preventing the recruiting of new members, foiling their attack plans.

- \textit{Protection / denial} is required should detection and prevention fail. It means hardening the target so that destruction or disruption becomes more difficult such as for example reinforced building structure, blast-resistant containers or redundant systems. It may include precautionary measures such as the deployment of manned guards.

- \textit{Interdiction} or \textit{crisis management} seeks to detect and forestall an imminent attack by identifying and neutralizing perpetrators, and preventing them from bringing their violent operation to fruition, such as the deactivation of an improvised explosive device (IED).

- \textit{Response and recovery}, also known as \textit{consequence management}, means containing damages and casualties in the aftermath of an attack –by organizing emergency responses, public health measures and restoring critical functions– and increasing resilience.

- \textit{Forensics} refers to the ability to identify the perpetrators of an accomplished action and is essential to elicit the adequate response. It includes forensic science and other investigative techniques to analyse terrorist and criminal means which can aid to track and apprehend suspects, as well as to support the arrest and prosecution of individuals responsible of the illegal action.

In addition, an area known as \textit{preparedness} shall be considered. It involves all the planning, organising and training processes required to meet the above mentioned tasks.

Obviously, the main question now is how to limit the scope of the security industry. Which industries are related to the above mentioned sources of insecurity and the tasks to deal with them, and which industries should be considered outside the security industry?

2.6. Who is the security industry?

2.6.1. Difficulty to limit the definition of the security industry

Due to the high diversity of threats to society, technologies and security solutions, the security sector is composed of companies of a very varied nature, who sometimes only share the term \textit{security}. The security industry generates products as well as services, which can include locks and safes, fire and burglar alarms, electronic access control systems, electronic surveillance equipment, armoured and protected vehicles, guard equipment and garments, security fencing, and security consulting. Sometimes products have a very small supply chain, while in others they may require the integration of components from a large supply chain such as border and maritime surveillance systems. This reason explains the vertical disintegration of the industry and the increasing number of companies involved in the supply chain. Sometimes production is very large and standardised such as in-motion detectors, whilst in others, it is

\textsuperscript{22} Marti Sempere 2011, p. 4-5.
tailored to satisfy specific end customer demands such as a building intrusion detection systems. Sometimes products are sold directly to the customer, whilst in others, distributors play a key role in the supply chain. The technology used in security products is varied and includes amongst others construction, automotive, aerospace, textiles and garments, ballistics, electronics, and information and communications systems. Usually these products and services are not only applicable to security, but also to other activities. As such, these products have a dual use. For example, identity cards may be used for police identification but also to exert the right to vote. Video cameras may be used for surveillance but also for leisure. It might even occur that an intermediate company ignores the fact that its product is integrated and sold in the security market. In sum, the varied nature increases the difficulty of the analysis and the possibility to find a comprehensive definition for the security industry.  

A recent survey of companies active in the security sector of 2009 illustrates the wide variety of services and products involved in the security industry. We have included this overview in Annex 3. It at the same time illustrates the necessity to more clearly define the security industry for the purposes of our study.

2.6.2. Who does belong to the security industry?

The EU vision and the Department of Homeland Security (Bush, 2002) take a very broad approach when security issues are at stake. This suggests that the analysis of the sector, in order to be comprehensive, should address several kinds of threats and risks and should encompass both security products and services.

The Commission Action plan for an innovative and competitive Security Industry distinguishes broadly the following sectors, indicating that this list is not exhaustive:

- aviation security;
- maritime security;
- border security;
- critical infrastructure protection;
- counter-terror intelligence (including cyber security and communication);
- crisis management/civil protection;
- physical security protection; and
- protective clothing.

However, the differences in technologies, products and services cast doubts about the convenience and appropriateness of such a broad approach.

An attempt to narrow down the definition of the security industry for the purposes of the analysis presented here is the following. The two most relevant areas of insecurity are terrorism and organized crime. It is clear that the industry that addresses insecurity caused by terrorism and organized crime belongs to the security industry. This industry faces two important insecurity sources which are confronted with a set of products and services that are largely common. Moreover, such commonality extends to combat illegal immigration since

---

25 The Department of Justice and the FBI also play a relevant role.
border control is also an effective method to fight against terrorism and organized crime. Furthermore, many of the security techniques can be used to deal with cybercrime as well (password protection...).\textsuperscript{27} Hence, it would not be necessary to deal with cybercrime and border control separately.

The industry related to natural (floods, hurricanes, earthquakes, forest fires) or manmade disasters (technological or industrial accidents usually known as safety industry) addresses the response to hazards that cause damage without purposeful action. Whilst the same kind of equipment is shared for mitigating damages originated by terrorism and organized crime, the preventive means are of a very different nature (e.g. weather prediction systems). Principal customers of this industry are more closely related to health, civil protection and environmental protection agencies rather than law enforcement. Yet, in the framework of this study only the industry producing goods that can be used for mitigating damages by terrorism and organized crime should be considered as ‘security industry’.\textsuperscript{28}

Public health may also be a target of terrorism or organized crime as another means to achieve desired goals. Chemical or biological agents can be dispersed in the air or water, infecting thousands of people, contaminating soils, buildings and transport assets, destroying agriculture, infecting animal and plant populations, and affecting food and feed at any stage in the supply chain. Safeguarding the society from this risk is a major challenge, where early detection systems and the pharmaceutical industry can provide some solutions.\textsuperscript{29}

In short, if the definition of the security industry has to be narrowed down, the industry that directly provides specialized goods and services to deal with insecurity caused by terrorism or organized crime in the following areas: aviation security, maritime security, border security, critical infrastructure protection and physical security protection can be considered as the ‘security industry’ in the framework of this study.

Yet, it may not be forgotten that other industries (e.g. pharmaceutical industry) can provide useful solutions. The question however is, whether these ‘side- industries’ should be considered as part of the ‘security industry’. To be very clear: the narrowing of this definition of the “security industry” is merely done for the purposes of the research within this project. The problem is that potentially the “security industry” can be interpreted very broadly, and without some attempt to narrow down its scope, it would be impossible to provide focused answers to the research questions central to this project. However, it should be remembered that the definition presented here (by mainly focussing on terrorism and organized crime in particular areas) is narrower than the definition provided in the Commission action plan. At the same time, the mere fact that the primary focus may be the security industry aimed at dealing with insecurity caused by terrorism and organized crime does not mean that the report merely has importance for those areas. First of all, we will in some cases look at other areas as well. E.g. in chapter 4, dealing with legislation and case law in the Member States, some of the cases we use clearly go beyond the narrow definition we provide here. Moreover, even though academically it is easier initially to work with a narrow definition of the security industry, some of the conclusions from this project can easily be transferred to areas belonging to a broader definition of the security industry and hence have relevance for the security industry as a whole.

\textsuperscript{27} Martí Sempere 2010, p. 5.
\textsuperscript{28} Martí Sempere 2010, p. 5.
\textsuperscript{29} Martí Sempere 2010, p. 8.
2.6.3. Fuzzy boundaries

Even when narrowing the scope of this industry, the difficulty to set clear boundaries remains, and may be a source of controversy.

There are some fuzzy boundaries. Take, for example, the industry related to the restoration and recovery of the situation to pre-event levels. This task involves long term activities that do not differ essentially from routine activities of maintenance, repair, reconstruction or upgrade. Hence, a criterion is required to set the scope, being a reasonable principle to consider only the industry related to the emergency activities performed in the aftermath of a security incident.\(^\text{30}\)

Similar problems appear when a distinction between products and services related to organised and ordinary crime is attempted. Since operating methods and countermeasures are alike –organised crime being perhaps more sophisticated and on a larger scale–, a real distinction cannot be settled and so it seems rational to consider the industry that faces both types of illegal activities as unique.\(^\text{31}\)

Moreover, suppliers are often specialised divisions of firms whose business is neither focused on security nor security is their main source of income. In such cases, within the proposed definition, these companies can be considered part of the security market as long as they manufacture products and services used to counter terrorism and organised crime. Companies that only provide some subsystems and components that cannot operate autonomously should in principle be considered outside this sector. Yet, in certain cases attention should be paid when these companies provide key components with few applications in other markets.\(^\text{32}\)

Diseases and pandemics are other major life risks that are confronted with the support of the health industry. This industry is related to terrorism and organised crime inasmuch it endows essential support to prevent and restore any damage to health and life. Yet, products and services provided by this industry do not markedly differ from those aimed at protecting the population against injuries, illnesses or pandemics caused by hazard. Although this industry should be considered outside this sector, the analysis of its capabilities to defeat attacks against public health, such as a chemical or biological attack, is of interest from a security point of view.\(^\text{33}\)

The industry related to the protection against natural disasters – such as floods, storms, droughts, earthquakes, forest fires – or unintentional man-made disasters – such as technological or industrial accidents –, usually known as the safety industry, shares many goods and services for mitigating damages which are also used for combating terrorism and organised crime. Nonetheless, the preventive means are of a very different nature as for instance weather forecasting systems, forest fire detection systems, watersheds for flooding prevention, and so on. Yet, unless these products are used for the combat of terrorism or organised crime, it should not be considered as ‘security industry’.\(^\text{34}\)

With respect to the defence industry, a special remark should be made. The difficulty in distinguishing between internal security, mainly related to the fight against terrorism and organised crime, and external security, mainly related to defence from other nations, poses additional challenges in qualifying suppliers to both industrial sectors. In effect, certain

\(^\text{30}\) Marti Sempere 2011, p. 6-7.
\(^\text{31}\) Marti Sempere 2011, p. 6-7.
\(^\text{32}\) Marti Sempere 2011, p. 6-7.
\(^\text{33}\) Marti Sempere 2011, p. 6-7.
\(^\text{34}\) Marti Sempere 2011, p. 6-7.
suppliers may be powerful enough to raise small armies and count with the support of certain states. Moreover, especially risky events—such as Olympic Games, World Cups and internal security incidents with far-reaching consequences—generally demand the (spare) capabilities of armed forces when civilian capabilities become insufficient as for example building temporary bridges or deploying campaign hospitals. However, **a rational criterion would recommend to incorporate in the definition of the security industry only that industry that does not supply what is traditionally considered military equipment.**

Finally, insurance companies play a relevant role in the security field, since they allow the transfer of the residual risk which cannot be mitigated with other types of investment. These companies provide insurance against potential damages, supplying financial support for incident recovery. Based on the estimated risk and consequences of undesired events, they set the payable amount (premium) for covering the economic losses of these events. Insurance companies may have a considerable influence in setting security standards and as a consequence in the demand of security products and services, since they provide deductions to customers that have invested in cost-effective loss-mitigation measures. However, **inasmuch these companies do not provide true solutions for either reducing or eliminating threats, they must be considered outside the scope of the security industry.**

### 2.6.4. Closely related industries and markets

The capability of some security products and services to indistinctly face defence, natural and man-made disasters, safety and other social needs as well as the similarity of development and production methods explain that security firms usually operate concurrently in these markets, insofar such strategy provides advantages in terms of a diversified customer base as well as synergies and economies of large production. This is the case for the following industries:

- **The defence industry**, because it shares common user needs in areas such as surveillance, communications and operation management systems, mission vehicles, or small arms to neutralise terrorist and criminals when they oppose resistance to law.
- **Building monitoring and management industry**, because it usually integrates fire protection, access control, or intrusion detection systems in addition to heating, air conditioning and other building controls.
- **Plant automation and control industry**, since it shares related technologies based on sensors, communication devices and control systems.
- **Scientific instrumentation industry**, where equipment such as X-ray, computer tomography, radiological detectors and so forth, facilitate certain inspection processes.
- **The ICT industry**, because it provides general purpose hardware, software and communications that it is integrated in many security solutions.

### 2.6.5. Comparison with the US

The Act that is often mentioned in the Invitation to Tender as the example of a liability regime regulating the safety industry, the US Safety Act, has a relatively limited scope by focusing strongly on technologies aimed at the prevention of terrorism. The Invitation to Tender of the European Commission clearly has a much broader scope, but this shows that

---

35 Marti Sempere 2011, p. 6-7.
36 Marti Sempere 2011, p. 6-7.
38 See on the US Safety Act Chapter 7 below.
the definitional issue should surely be addressed in an early stage of the project. The above proposal suggests to limit the security industry as follows: ‘the industry that directly provides specialized goods and services to deal with insecurity beget by terrorism, organized crime, border security, cybercrime and critical infrastructure protection can be considered as the ‘security industry’.

2.7. Conclusion

The perceived risks by EU citizens included terrorism and organized crime, but also cybercrime, border security and natural and nuclear disasters. For the purpose of this study, it might however be appropriate to limit the perceived risks to terrorism and organized crime, in particular in relation to facilities such as airports, train stations, etc. as this arguably is the main rationale of this study. Terrorism is special because it involves the intentional causing of large damage, and terrorists, in a rather natural sense, ‘compete’ with the security industry.

Arguments not to include the other perceived risks are the following: cybercrime is outside the scope because it cannot directly cause physical damage, border security is more an economic issue, and natural and nuclear disasters do not involve intentional damage-causing. Furthermore, the proposed definition in the European Commission Action Plan for an innovative and competitive Security Industry covers the industry that produces products to deal with:

- aviation security;
- maritime security;
- border security;
- critical infrastructure protection;
- counter-terror intelligence (including cybercrime and communication);
- crisis management /civil protection;
- physical security protection;
- protective clothing.

Yet, this definition is still very broad. It might therefore be hard to focus on the crucial security risks, being terrorism and organized crime.

We therefore propose the following definition of the security industry in the framework of this study:39

1. The security industry is defined to include “providers of products and services that are specifically intended to reduce the risks of intentional damage caused by terrorism and organized crime in the following areas:

- aviation security;
- maritime security;
- border security;
- critical infrastructure protection;
- physical security protection.

2. The following products and services are regarded as provided by the security industry:

39 The reader should keep in mind what was mentioned at the end of section 2.6.2: this definition is merely adopted for the purposes of this study and we certainly do not argue that the concept of the security industry should at a policy level be narrowed down to our definition.
scanning and detection equipment for use with passengers and cargo (or other goods) at airports, train stations, ports, power plants, and similar large facilities, including products and services for weapons and explosives detection, chemical and biological risk detection, and radionuclide detection.

3. The following industries are NOT part of the security industry for the purposes of this report:
   - defense industry;
   - building monitoring and management industry;
   - plant automation and control industry;
   - scientific automation industry;
   - ICT industry, software, information technologies;
   - other providers of products and services that are not specifically intended to reduce the risks of intentional damage caused by terrorism and organized crime, such as providers of fences, reinforced glass, etc.”.

The above conclusions with respect to the security industry are visualized in the graph below.
The security Industry

Perceived risks
- Terrorism
- Organised Crime

Tasks of the security industry
- Preparedness
  - Consultancy
  - Training and rehearsal
  - Intelligence and Surveillance
    - Closed Circuit Television (CCTV)
    - Intrusion detection and perimeter protection
    - Border protection
    - Identification and access control
    - Goods and merchandise
    - Intelligence systems
    - CBRN detection equipment
    - Other awareness products
- Protection (critical infrastructure protection)
  - Building protection
  - Vehicle protection
  - Personal protection
  - Manned guarding services
  - Information systems protection
- Interdiction and crisis management
  - Personnel equipment, e.g., surveillance gear
  - Surveillance vehicles
- Response and recovery
  - Firefighting
  - First response health care
  - Logistic support
  - Coordination and management
- Forensics
  - Laboratory equipment
  - Investigation services

Who is the security industry
- Industry that produces products to deal with:
  - Aviation security
  - Maritime security
  - Border security
  - Critical infrastructure protection
  - Physical security protection
- Closely related industry (but not security industry)
  - Defense industry
  - Building monitoring and management industry
  - Plant automation and control industry
  - Scientific automation industry
  - ICT industry
- Non-limited list of security services
  - Scanning and detection equipment for use with passengers and cargo (or other goods) at airports, train stations, ports, power plants, and similar large facilities, such as:
  - Weapons and explosive detectors
  - Radionuclide detection equipment
  - Chemical and biological risk detection
Chapter 3 Analysis of comparable EU legislation

A first approach to tackle a possible liability regime for the European security industry is to simply analyse potential analogies to third party liability for security related products and services in primary and secondary EU law. Hence in this chapter, subdivided in five sections,\(^{40}\) we will examine various European directives such as the Product Liability Directive, the General Product Safety Directive and the Environmental Liability Directive, as well as particular regulations, with the goal to analyse potential analogies to third party liability for security related products and services. As we made clear in the introduction where the methodology was explained\(^{41}\) in this chapter we will on the one hand examine to what extent the relevant EU legislation we will examine could be applied to security related products or services; on the other hand we will also analyse to what extent particular legislative solutions we come across in current EU legislation may constitute an interesting example for a potential special liability regime for the EU security industry. As also indicated in the methodology in the various subsections where the EU legislation is analysed we try to follow a similar structure on the basis of the common format for analysis of liability and regulatory regimes.\(^{42}\)

This analysis of comparable EU legislation will mostly consist of an analysis of legislation rather than an analysis of case law. The simple reason is that at the EU level cases could only come from the EU Court of Justice. With the exception of the Product Liability Directive, European case law in this domain is in fact extremely limited. Moreover, even in the area of the Product Liability Directive there is case law, but most of it is not relevant for the issues central to this study. Hence, where relevant we may occasionally refer to a case, but our discussion of case law will be limited. One reason for the fact that there is not much European case law is that the European legislation (to be discussed in this chapter) is implemented in Member States law. There may obviously be cases in the different Member States. Case law will therefore be discussed in more detail in chapter 4 dealing with Member States law.

3.1. Environmental Liability Directive 2004/35/EC\(^{43}\)

3.1.1. Brief summary of the regime

With the Environmental Liability Directive (hereafter Directive or ELD), the Community aims to establish a framework of environmental liability based on the ‘polluter-pays’ principle, to prevent and remedy environmental damage.\(^{44}\) The Directive covers water pollution, damage to biodiversity and land contamination.\(^{45}\)

The liable party is in principle the "operator", i.e. the natural or legal person who carries out an occupational activity. Based on the polluter pays principle, the directive imposes strict liability on operators of risky or potentially risky occupational activities, which are listed in the annex of the directive. Fault liability applies to operators of non-listed activities, but only

\(^{40}\) The five sections obviously correspond to the different tasks of Work Package 1 of the Invitation to Tender.

\(^{41}\) See supra 1.4.

\(^{42}\) Included in Annex 1.

\(^{43}\) This corresponds to Task 1.1 of Work Package 1 of the Invitation to Tender.


\(^{45}\) ELD, Article 2.
for damage to biodiversity. Operators have to take the necessary preventive action in case of imminent threat of environmental damage. They are also obliged to remedy the environmental damage once it has occurred. In specific cases where the operator fails to do so or is not identifiable, the competent authority may carry out the necessary preventive or remedial measures. Remediation has to consist in the remediation of the damaged natural resources (nature, water, soil) to or towards the "baseline condition" (restoration in kind or - if not or not completely possible - by recreation of similar resources).

Members States do have the possibility to enact more stringent provisions in relation to the prevention and remedying of environmental damage. ELD liability cannot be limited or excluded by contract.

3.1.2. Basis of liability

The ELD imposes obligations on operators to prevent environmental damage and if necessary to remedy it and to report threatening or actual damage to the authorities. The government has the authority to order the operator to take additional measures to prevent or to remedy environmental damage. If the operator does not comply, the competent authority can execute the measures, or have them executed by a third party and recover the cost from the operator.

The Directive provides for two distinct liability regimes: a strict liability regime and a fault liability regime. First, strict liability applies to operators who professionally conduct risky or potentially risky activities. These activities are listed in Annex III of the Directive. The strict liability regime covers damage to protected species and natural habitats, water and land damage. Second, fault-based liability applies to all other professional activities. Unlike strict liability, this regime only applies to protected species and natural habitats, not to water or land damage.

As such, the ELD does not offer a real civil liability regime, but a mainly public law regime to be enforced by competent authorities, combined with private law aspects as strict liability and fault-based liability. Through this mechanism the ELD should ensure that the polluter-pays principle enshrined in Art 174 (2) of the EC Treaty is realised.

3.1.3. Liable persons (attribution of liability)

A site operator who caused environmental damage can be held financially liability under the ELD.

The term ‘operator’ is defined as any natural or legal, private or public person who operates or controls the occupational activity or, where this is provided for in national legislation, to
whom decisive economic power over the technical functioning of such an activity has been delegated, including the holder of a permit or authorization for such an activity or the person registering or notifying such an activity. Occupational activity is defined as any activity carried out in the course of an economic activity, a business or an undertaking, irrespectively of its private or public, profit or non-profit character.

There are a few cases in which operators can be exempted from liability. Exemptions can be found in Article 4 of the Directive and include for example act of war, force majeure and environmental damage that falls under the scope of international conventions listed in Annex IV. Besides these exemptions, the Member States may adopt a partial or a complete state-of-the-art defence or permit compliance defence (see under 5 below).

If the operator is unknown (so-called ‘orphan sites’), it follows from Article 5 §4 and Article 6 §3 of the ELD that the authorities are not obliged to take preventive or remedial measures themselves. This might somewhat be compensated by the wording of Article 8 § 2, which stipulates that the competent authority shall recover, inter alia, via security over property or other appropriate guarantees, from the operator who has caused the damage or the imminent threat of damage, the costs it has incurred. In this sense, Article 8 §2 addresses aims to protect the competent authority against insolvency of the operator. Moreover, several of the Directives to which the ELD refers to, contain obligations requiring the authorities to take remedial measures. Article 4 §4 of the Wild Birds Directive and Article 6 §2 of the Natural Habitats Directive require Member States to take appropriate measures to avoid pollution. The Water Framework Directive obliges Member states in Article 4 §6 to ensure that all practical measures are taken with the aim of restoring the body of water to its status prior the incident. Moreover, the Member States may be held liable under the Frankovich doctrine if they have committed a serious breach of the Environmental Liability Directive, for example if they failed to oblige to operator to take preventive or restorative measures.

If there are multiple liable parties the ELD refers to national legislation: ‘the Directive is without prejudice to any provisions of national regulations concerning cost allocation in cases of multiple party causation, especially concerning the apportionment of liability between the producer and the user of a product’. Data on the transposition of the ELD in the Member States show that most Member States adopted joint and several liability. Joint and several liability puts a higher burden on the operators, but possibly Member States have made this choice in order to guarantee that the ‘polluter pays’-principle would be guaranteed.

Member States have to ensure that effective means of implementation and enforcement are available. The Member States therefore have to designate the competent authority(ies) responsible for assessing the significance of the damage and determining which remedial measures should be taken.

---

51 ELD, Article 2(6).
52 ELD, Article 2(7).
53 ELD, Article 8, § 4.1 (permit defence) and Article 8, § 4.2 (state-of-the-art defence).
54 Article 5, § 4 on preventive action states that if the operator fails to comply with his obligations, cannot be identified or cannot bear the costs, the competent authority may take these measures itself. Article 6, § 3 states the same for remedial action.
55 Krämer 2005. See also Bocken 2006.
56 The Wells judgement (Case C-201/02) made clear that public authorities can incur state liability for failure to apply EC environmental law.
58 ELD, Article 9.
59 De Smedt 2009.
60 ELD, Article 11, § 1 and Preamble 24.
A qualified (environmental) NGO or another natural or legal person may submit comments concerning environmental damage or an imminent threat of environmental damage to the relevant competent authority and request the authority to take action under the ELD. 61

3.1.4. Damage covered

Environmental damage in terms of the Directive includes damage to protected species and habitats, water damage and land damage. 62 Yet, damage to protected species and habitats is limited to species of birds listed in the Wild Birds Directive 63 and their habitats and those listed in the Habitats Directive 64 and any other habitat or species so determined by a Member State. 65 The first two categories are also known as Natura 2000 sites, which covers approximately 17% of the Community’s land area. Consequently, harm to ‘unprotected’ species and habitats falls outside the scope of the Directive. Annex I of the Directive provides a list of criteria to determine when there is damage to protected species and habitats.

Water damage only falls within the Directive’s scope if the water-course is covered by the Water Framework Directive (Directive 2000/60/EC) 66 and the Directive is only applicable to land contamination if there is a significant risk that human health is adversely affected. 67 Hence, land contamination in uninhabited areas will fall out of the scope of the Directive.

Traditional damage, such as damage to health and property, has been excluded from the scope of the Directive. Furthermore, the Directive does not apply to damage occurred before 30 April 2007 or damage that occurred more than 30 years ago. 68

3.1.5. Exclusions and defences

The ELD allows the Member States to include operator defences. Article 8(3) stipulates that the operator shall not be required to bear the cost of preventive of remedial actions if he can prove that the damage was caused by a third party intervention or because the damage resulted from compliance with a compulsory order (article 8(3)).

Article 8(3) and in particular damage caused by third party could be relevant for the security industry. Under the proposed ELD, this defence was subject to the additional condition that the third party intentionally caused the damage. The final wording of Article 8, however, does not impose this condition. An operator that can invoke the defence is exonerated from financial liability, if he can show that appropriate safety measures were in place. Relevant third party acts include negligent and intentional acts, as well as any other acts. In all of these cases, the operator is the victim of a third party act, and, if appropriate safety measures were in place, he may be completely blameless and the damage-causing event may have been entirely beyond his control.

---

61 ELD, Article 12.
62 ELD, Article 2.
65 ELD, Article 2, § 3c.
67 ELD, Article 2, § 1c.
68 ELD, Article 17.
The ELD does not define the term ‘third party’. In any event, persons, both natural persons and legal entities, that are not related to the operator and access the operator’s site with authorization are covered by this term. This includes terrorists and other criminals. Employees, on the other hand, are likely not third parties, and, thus, if an employee acting outside the scope of his authority causes environmental damage, the company cannot invoke the defence. In some cases, however, employees could qualify as third parties, such as where an employee causes a bomb to explode at the facility over the weekend.

If the operator has a contract or business relation with the putative third party, the defence may or may not be available. A maintenance service provider that performs services solely for one company (i.e. as it were an employee) may not be considered a third party. The polluter pays principle suggests that the concept of third party should not be interpreted restrictively: if the third party under contract with the operator causes environmental damage, there is no reason to reject the defence and treat the operator as the polluter. Note, too, that even if the operator cannot invoke the defence, it may still have a claim against the third party that actually caused the damage under contract or civil law.

The condition that appropriate safety measures must be in place for the defence to be available, raises the issue how far the requisite safety measures should go. The operator should in any event implement the safety measures required by law, regulations, and the permits for the facility. Whether he should go beyond this minimum needs to be analysed on a case-by-case basis. If the safety measures required by law are onerous and are aimed at establishing a high level of safety, there would appear to be no reason to raise that level further for purposes of the defence. Industry standards and best practice may also play a role in this assessment. The potential for terrorist acts to cause damage, on the other hand, is not an independent factor in determining the safety measures required for the defence to apply.”

Besides the defences provided in Article 8(3), the Directive allows for a permit and/or a state-of-the-art defence (article 8(4).

Article 8 (4) of the ELD states that ‘Member States may allow that operators do not have to bear the cost of remedial actions if he demonstrates that he was not at fault or negligent and that the environmental damage was caused by an emission or event expressly authorised by, and fully in accordance with the conditions of, an authorisation conferred by or given under applicable national laws and regulations which implement the legislative measures adopted by the Community specified in Annex III, as applied at the date of the emission or event’. Hence, the permit defence would be available to the operators of dangerous occupational activities listed in Annex III of the Directive. Normally, strict liability would apply to these operators.

The Directive also allows Member States to include a state-of-the-art defence. A state-of-the-art defence holds that an operator should not be liable if his activities were not considered to cause harm according to the state of scientific and technical knowledge at the time of the activity.

The ELD stipulates in Article 8 (4) (b) that ‘where an emission or activity or any manner of using a product causes damage and the operator demonstrates that scientific and technical knowledge at the time when the emission was released or the activity took place did not consider it likely that such damage would occur, Member States may allow the operator not to bear the restoration costs’.

69 ELD, Article 8(4).
70 See also Wenneras 2005b, p. 153.
71 ELD, Article 8(4).
Note that the ELD requires the operator to demonstrate that he complied with the permit or that the risk was unknown at the time of the accident.\textsuperscript{72}

The possibility to include a permit or state-of-the-art defence was among the most contentious issues in the ELD debate. Indeed, in theory, strict liability could be a strong incentive for operators of dangerous activities (annex III operators) to take all possible risk-minimising measures and it could be a way of implementing the precautionary principle. Yet, with a permit defence, there might not be a strong incentive for the potential liable operators to invest in risk-minimising measures as with a permit defence, the operator could be exempted from liability because he complied with the permit.

The permit defence and the state-of-the-art defence probably are also relevant defences for the security industry. However, it must be emphasised that the latter defence only can be advanced if the most advanced objective state of scientific and technical knowledge did not enable the producer to detect the risk.

3.1.6. Causation

According to Article 5 (1) and Article 6 (1) of the ELD, the operator is obliged to take the necessary preventive or remedial measures in case damage might occur or has occurred. Yet, the preventive and remedial measures obliged in Articles 5 and 6 of the ELD require a causal relationship between the operator and the (potential) damage.

The ELD is rather vague with respect to causation. From the Directive it cannot be read immediately whether the burden of proof of the existence of a causal relationship lies with the operator or with the authorities who make allegations of damage. The common practice is that the burden of proof lies with the plaintiff, which in the case of the ELD would be the authorities. This practice seems to be followed by the ELD as the Articles 3(1) and 4(5) of the ELD limit the application of the Directive, whereas Article 8(3) and (4), concerning permit defence and state-of-the-art defence clearly reverse the burden of proof on the operator.\textsuperscript{73}

It might be wondered whether the causality requirements, as far as they can be deducted from the wording in Articles 3(1) and 4(5) of the ELD could prevent that operators would be held liable for the damage they caused. Indeed, the most problematic issue in liability regimes is precisely the causality requirement. A strict application of full proof of a causal link between the damage and the operator might paralyse the liability regime.\textsuperscript{74} This might even be more relevant in the case of environmental liability as environmental damage might be caused by multiple sources so that it might be difficult to retrieve the main polluter.

Yet, from Article 4 (5) ELD follows that the ELD does not require a causal link between the damage and one single operator, as reference is made to ‘operators’. Nevertheless, as stated above, with respect to joint and several liability, the ELD passes the issue on to the Member States. Article 9 of the ELD states that if more than one operator causes environmental damage, the cost of remedying that damage is allocated among the operators according to the domestic law of Member States, in particular ‘the apportionment of liability between the producer and the user of a product’.\textsuperscript{75}

\textsuperscript{72} ELD, Article 8(3) and 8(4).
\textsuperscript{73} Wagner 2005, p. 90-91.
\textsuperscript{74} Wagner 2005, p. 91.
\textsuperscript{75} ELD, Article 9.
3.1.7. **Relation with (other) regulation**

The ELD was already amended twice through Directive 2006/21/EC on the management of waste from extractive industries and through Directive 2009/31/EC on the geological storage of carbon dioxide and amending several directives. The amendments broadened the scope of strict liability by adding the “management of extractive waste” and the “operation of storage sites pursuant to Directive 2009/31/EC” to the list of dangerous occupational activities in Annex III of the ELD.

On 27 October 2011 the Commission adopted a Proposal for a Regulation on safety of offshore oil and gas prospections, exploration and production activities. The Proposal also contains an amendment to the ELD (Article 37).

3.1.8. **Financial security and compensation mechanisms**

Article 14 of the ELD provides that ‘Member States shall take measures to encourage the development of financial security instruments and markets by the appropriate economic and financial operators, including financial mechanisms in case of insolvency, with the aim of enabling operators to use financial guarantees to cover their responsibilities under the Directive’. Pursuant Article 14(2), the Commission reviewed the situation in 2010, and examined whether the regime should be modified. If appropriate, the Commission could submit proposals for a system of harmonised mandatory financial security, but so far it has been considered too early to propose a harmonised mandatory financial security regime.

It appears that only a minority of the Member States did include a provision on obligatory financial guarantees in their national law. Eight Member States have introduced mandatory financial security entering into force at different dates up to 2014: Bulgaria, Portugal, Spain, Greece, Hungary, Slovakia, Czech Republic and Romania. These systems are subject to risk assessment of relevant sectors and operators, and dependent on various national implementing provisions providing for issues such as ceilings, exemptions, etc. However, mandatory financial security is delayed in all three countries where it was supposed to come into effect in 2010 (Portugal, Spain, Greece) because essential provisions were not yet in place. The remaining Member States rely on voluntary financial security.

In principle there is no financial limit on the amount that liable polluters will be required to pay to remedy environmental damage. The Directive, however, allows the public authorities in charge of its implementation to decide, on a case by case basis, to cap the liability of the responsible operator. This can be done when the remedial measures already taken ensure that there is no longer any significant risk of adversely affecting human health, water or protected species and natural habitats, and when the cost of the remedial measures to complete the restoration of the damaged environment would be disproportionate to the environmental benefits.

---

76 ELD, Article 14, § 1.
77 Report from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions under Article 14(2) of Directive 2004/35/CE on the environmental liability with regard to the prevention and remedying of environmental damage, COM/2010/0581 final of 12 October 2010, p. 4.
78 Report from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions under Article 14(2) of Directive 2004/35/CE on the environmental liability with regard to the prevention and remedying of environmental damage, COM/2010/0581 final of 12 October 2010, p. 4.
3.1.9. **Rules of evidence**

The authorities bear the burden of proof of the environmental damage and the causal link between the activities of the operator and the damage; the producer bears the burden of proof of the permit and/or state-of-the-art defences (see 6 above).

3.1.10. **Jurisdictional and procedural issues**

The ELD entitles the national competent authority to initiate cost recovery proceedings against the operator in relation to any measures taken in pursuance of the Directive within five years from the date on which those measures have been completed or the liable operator has been identified, whichever is the later.\(^8\)

The ELD does not address jurisdictional and procedural issues.

3.1.11. **Conclusions Environmental Liability Directive**

The ELD regime addresses environmental damage caused by occupational activities, and hence is only applicable to the security industry if environmental damage is caused.

Nevertheless, the ELD might provide insights relevant to third party liability of the security industry.

The ELD leaves significant discretion to the Member States which may not only decide on the use of optional defenses but also on other optional choices (scope regarding damage to nature, as regards the “operator”-definition, the type of multi-party causation, the forms and measures regarding financial security etc.). Member States may moreover adopt or maintain more stringent measures than prescribed by the Directive (Article 193 TFEU, Article 16(1) ELD).

From the transposition data it appears that the majority of the Member States does not go beyond the minimum requirements. The majority of the Member States does not extend the scope of the Directive, does not require financial guarantees and allows for a permit and/or state-of-the-art defence, without subsidiary state liability. This outcome is consistent with the liability regime as foreseen in the Environmental Liability Directive, as the flexibility in the Directive allows the Member States to implement their own preferences. However, this flexibility may make it harder for the Directive to fully realise the prevention and restoration of the environment, implement consistently the ‘polluter-pays principle’ and establish a level-playing field. Yet, the realisation of a level-playing field is an important item for the security industry, and hence, a liability regime that leaves major decisions to the Member States probably will not realise this aim. It will rather create uncertainty. Moreover, the subsidiarity principle (Article 5 EC Treaty) limits the legitimation of European lawmaking.

Furthermore, introducing a strict liability regime without obligatory financial guarantees might result in insolvency of the producers in the security industry. The evolving experience of the ELD with financial guarantees therefore should therefore certainly be taken into account when considering a liability regime for the security industry. Eventually, the development of specialised insurance products might be recommendable.

\(^8\) ELD, Article 10.
Finally, Article 8(3) of the ELD and in particular damage caused by third party could be relevant for the security industry. An operator that can invoke the defence is exonerated from financial liability, if he can show that appropriate safety measures were in place. Relevant third party acts include negligent and intentional acts, as well as any other acts. In all of these cases, the operator is the victim of a third party act, and, if appropriate safety measures were in place, he may be completely blameless and the damage-causing event may have been entirely beyond his control.

3.2. **Legal analysis of product-related EU legislation**

This task focuses on (1) EU legislation that (a) regulates products, including their effectiveness, their safety, and other properties, and (b) establishes liability for damage caused by products, and (2) related case law of the European courts. The relevant EU legislation includes general and sector-specific legislation.

The following EU legislation is analyzed in this section:

- **EU product-related liability regimes:**

- **EU product-related regulatory programmes:**
  - General Product Safety Directive (Directive 2001/95);
  - REACH and CLP Regulations (Regulations 1907/2006 and 1272/2008);
  - Plant Protection Product Regulation (Regulation 1107/2009);
  - EUDRALEX;
  - Personal Protective Equipment Directive (Directive 89/686);
  - Machinery Directive (Directive 2006/42); and
  - Construction Products Regulation (Regulation 305/2011).

These laws are diverse, have different objectives, and use diverging instruments to achieve their objectives. In general, they are aimed at (i) protecting safety, health, and the environment, and (ii) establishing an internal market without regulatory barriers by harmonizing product-related requirements. The instruments employed by these laws include the following:

*Informational and disclosure requirements*: Such provisions require that regulated entities provide information about the products to government agencies (e.g. through filings), consumers (e.g. through labels), and/or other parties. The information thus disclosed can inform further decisions, such as the government’s decision whether to intervene and impose further requirements or the consumer’s decision whether to purchase the product. Thus, informational requirements may result in changes to production and products even if the government does not intervene. If information is publicly available, it may be used to support claims against a regulated entity. On the other hand, public disclosure of information may shield a regulated entity from liability if the relevant risk was disclosed.

*Production or design requirements*: These provisions applicable to production or the products specify (i) the means that must be used in the manufacture or use of the product and/or (ii) the results to be achieved in manufacturing or in the products. We focus also on the role of

---

81 This corresponds to Task 1.2 of Work Package 1 of the Invitation to Tender.
European standards in the implementation of essential requirements applying to products. These requirements may play a role in defining the standard of liability for regulated entities.

*Registration, notification, or authorization requirements:* These provisions require more than the disclosure of information. Typically, regulated persons are required to submit a registration or notification, or seek authorization, before they may place a specific product on the market (or use it). These requirements may be relevant to doctrines such as the regulatory compliance defense.

*Post-marketing monitoring and reporting requirements:* These provisions require that regulated persons monitor product performance, in particular its adverse effects, after it has first been placed on the market. In some cases, reporting to government agencies may be required. On the basis of this information, the government may seek to intervene. In addition, these requirements may affect liability exposure by reducing the number of incidents, making information available to support claims, etc.

*Warning or recall obligations.* If performance, safety, or other issues are discovered post-marketing, regulated entities may be required to issue warning to users of the products concerned. In some cases, they may be required to recall the products concerned. Warnings and recalls tend to reduce liability exposure.

In addition to the instruments used by these regulatory regimes, the other subjects set forth in the common format are discussed for each regulatory program covered by this study.

### 3.2.1. Product Liability Directive 1985/374

#### 3.2.1.1. Brief summary of the regime

The Product Liability Directive\(^2\) (PLD), as amended by directive 1999/34,\(^3\) harmonizes the laws of Member States on product liability. It imposes on manufacturers liability for certain kinds of damages caused by defective products.

The term ‘product’ is defined as ‘all movables even if incorporated into another movable or into an immovable’. This definition covers security products. It does not cover services, even when provided in connection with products, such as healthcare professionals using a defective medical device with a patient,\(^4\) or security services provided at an airport or train station.

Liability is imposed when a defective product causes death, personal injury, or damage to private goods. The PLD sets forth certain defences, including the so-called ‘development risk’ and the ‘compliance’ defences.

PLD liability cannot be limited or excluded by contract.

---


\(^4\) Case C-495/10 Centre hospitalier universitaire de Besançon v Thomas Dutrueux [2011] ECR I-00000.
3.2.1.2. Basis of liability

PLD liability requires a defect that causes damages (PLD, Art 1). Thus, it does not explicitly require fault and, in that sense, is a non-fault regime, although the concept of defect implies notions of shortcomings.

A product is defective ‘when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation’ (PLD, Article 6(1)). A product may be deemed defective even if the defect is unavoidable, e.g., a human blood contaminant that cannot be detected.\(^{85}\)

A security product could be deemed defective under this definition if it suffered from a design defect, a manufacturing defect, or an informational defect. With respect to the design of security products, an issue arises as terrorists are trying to circumvent or ‘out smart’ the existing technology. This raises the question of whether the design of a security product is defective if it does not protect against the latest terrorist technology or practice. For a discussion of the defence regarding defects not existing at the time the product was put into circulation and the development risk defence, see under 5, below. Of course, a security product may also be defective because one of its component is missing (a manufacturing defect) or because it is not accompanied by the instructions needed to use it properly (an informational defect).

The product’s defectiveness is not determined based on the expectations of the victim, but on those of a representative of “the public-at-large or of an average consumer of the particular product.”\(^{86}\) Determining what the expectations are of the public-at-large with respect to security products may be complicated. The public-at-large may have high expectations for security equipment to protect them against security risks, including terrorist attacks. Producers of such equipment, however, do not typically have well-developed channels of communication with the general public, unlike, for instance, an electronics manufacturer, which can manage expectations through, for example, a user manual. Although producers of security products could label their products, there is a question about how effective this would be in shaping and influencing expectations. The customers for security products may also be wary about informing the public of the details of the detection capabilities and limits of security equipment for reasons of not assisting criminals and terrorists or not stirring up concerns among the public.

The assessment of whether a product is defective must be made at the time it is put into circulation (for further discussion, see under 5, below). It is irrelevant that a “better” product is subsequently put into circulation (PLD, Art 6(2)).

The PLD does not prevent the application of national liability regimes based on other principles (such as negligence, or dangerous goods). Article 13 of the PLD provides that it does not affect existing national liability rules. Under national law, a victim may thus have a choice to pursue a claim under the PLD-transposing legislation or under another national liability regime, whichever is more favourable.

There is no requirement that the product be provided to the person that suffered the damage. A producer of a security product could, for example, be held liable by a person that suffered

---

\(^{85}\) A & Others v National Blood Authority [2001] 3 All ER 289.

\(^{86}\) Hunter and Bergkamp 2001, p. 403, 404.
injury due to a defective detection machine not detecting explosive material that it was
designed to detect.

PLD liability cannot be limited or excluded by contract, but it can be supplemented by
contract. A supply contract, for example, could provide that the producer is liable for
economic damages caused by a defective product, even though the PLD does not cover such
damages. In sectors of industries where customers have strong bargaining power, producers
can effectively be required to assume liability that extends beyond the PLD.

3.2.1.3. Liable persons (attribution of liability)

Producers and importers of products are liable under the PLD regime (PLD, Art 1). The term
‘producer’ is defined as any producer of a finished product, raw material or component, as
well as any person putting his brand on the product (PLD, Art 3(1)). Producers of components
are thus liable under the PLD regime, but they can invoke certain specific defences (see under 5,
below), including that the defect is due to instructions provided by the producer of the
finished product.

The term ‘importer’ covers “any person who imports into the Community a product for sale,
hire, leasing or any form of distribution in the course of his business” (PLD, Art 3(2)).

If the producer or importer is unknown, the PLD provides that the supplier of the product may
be held responsible, unless it identifies its supplier or the producer or importer within a
reasonable time. The supplier may not otherwise be held liable.87

If there are multiple liable producers (for example, the producer of the finished product and
the producer of one of the components), they will be jointly and severally liable. In other
words, each one is liable for the full amount, but a person paying part or all of this amount
may have contribution claims against other liable persons.88 In the case of damages caused by
a defective security system (e.g., failure to detect explosives), the producers of the products
(or components) making up this system could be jointly and severally liable. If covered
damage is caused both by a defective security product and an improper use by a security
guard, the producer of the security product is fully liable under the PLD; any recourse or
contribution from the security guard is governed solely by national law.

If, however, the victim or a person for whom it is responsible is negligent, the liability of the
producer may be reduced or even disallowed (PLD, Art 8(2)). A victim will likely not be
deemed negligent based on the fact that he entered a public place; whether a victim might be
deemed negligent if he/she ignored general warnings, or even a specific security warning, is
an open question. A naive airline passenger accepting a suitcase from a terrorist, might be
regarded as negligent, however.

The PLD does not set forth rights of contribution or recourse, which are left to the laws of the
Member States. Where the damage is caused by a terrorist act, the terrorist will likely be
liable under national liability law, but recourse is unlikely to result in recovery.

87 Case C-402/03 Skov Æg v Bilka Lavprisvarehus A/S and Bilka Lavprisvarehus A/S v Jette Mikkelsen and
88 Hunter and Bergkamp 2001, p. 403-404.
3.2.1.4. Damage covered

The PLD covers only the following damages (PLD, Art 9):

“(a) damage caused by death or by personal injuries;
(b) damage to, or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 EUR, provided that the item of property:
(i) is of a type ordinarily intended for private use or consumption, and
(ii) was used by the injured person mainly for his own private use or consumption.”

The PLD does not cover other damages, such as pain and suffering, economic and environmental damages, but it does not prohibit that Member State national law cover additional types of damages. Thus, under the PLD, the producer of a defective product is not liable for non-material damages or damages to professional property, such as property of an airport or an airline, but it could be fully liable for personal damages and damage to private properties. The liability exposure is unlimited, unless the Member State concerned has adopted a liability cap.

The PLD allows Member States to adopt a liability cap of at least EUR 70 million for personal injuries caused by mass-produced products (“identical items”) with the same defect (PLD, Art 16(1)). Any such limit would likely apply to only some security products (such as, possibly, alarm systems or bullet-proof vests).

3.2.1.5. Exclusions and defences

The PLD provides several defences and grounds for exoneration.

The producer is not liable if he proves (PLD, Art 7):

“(a) that he did not put the product into circulation; or
(b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; or
(c) that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business; or
(d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or
(e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered; or
(f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.”

89 Both Germany and Spain have adopted such a liability cap. In Germany, the cap for cases of personal injury in respect of the producer’s overall liability across cases arising from the same defect, is set at € 85 million. The German Drug Act sets a ceiling of €120 million and €7.2 million p.a. (for annuities) and cuts individual claims at a maximum of €600,000 (€36,000 p.a. for an annuity). The German Genetic Engineering Act has a total limit of €85 million. There are no specified limits in tort or contract. Spanish legislation lays down a maximum of €63,106,270.96 for recoverable damages as a manufacturer’s global liability for death or personal injury caused by identical products causing the same defect. Greece and Portugal did have a liability cap in place but later removed it.
The defence under (e) is known as the “development risk” defence. Member States are not required to provide the development risks defence in their national law (PLD, Art 15(1)).

The producer may also be partly or totally exonerated from liability if he shows that the damage is caused both by a defect in its product and the fault of the injured person or any other person under his responsibility (PLD, Art 8(2)).

The most relevant defences for the security industry are the compliance defence (for further discussion, see under 7, below), the defence that the defect did not exist at the time when the product was put into circulation, and the development risk defence. This defence is available only if the most advanced objective state of scientific and technical knowledge did not enable the producer to detect the defect. It is not sufficient to prove that there was no known methods of detection within the industry. In the security industry, knowledge may rest with the industry, but also the public authorities. Such knowledge, however, may not be publically available, or not even to all security products providers, for security reasons.

A claim that could be made in connection with a terrorist attack is that the design of the detection equipment involved should have enabled a particular risk to be detected (e.g., an airport security detection system should detect thin layers of a new type of explosives hidden in books). The PLD does not treat as defective a security product that could not detect a risk (e.g., a particular method used by terrorists to hide explosives) that was unknowable and undetectable at the time the product was put into circulation.

The availability of the development risk defence in the case of known but undetectable risks is less certain. In the UK, a court ruled that the supplier of blood contaminated by a known infectious agent was liable for the ensuing damage, even though this agent was undetectable. A Dutch court adopted a different position in a similar case involving the HIV virus that could not be detected in the particular blood product that was contaminated.

3.2.1.6. Causation

The PLD does not provide any specific rule regarding causation. This issue is left to the Member States.

The only requirement is that the damage was ‘caused by’ the defective product. It is generally recognized in the literature that a defective product can ‘cause’ damage actively (i.e., by transmitting a virus) and passively (i.e. by not providing a benefit that should have been provided, e.g., a vaccine that does not work). Thus, a security product can be found to have ‘caused’ damage if it failed to detect a risk.

---

90 All Member States have done so, except Finland and Luxembourg. Certain products are also excluded from this defence in France (human blood and derivatives) and Germany (medicinal products and GMOs).
91 “The defence cannot be satisfied simply because the standards precautions in the interested industrial sector had been complied with. (…) the producer of a defective product must prove that the objective state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation was not such as to enable the existence of the defect to be discovered.” See Case C-300/95 Commission v United Kingdom [1997] ECR I-02649, 25 and 29. For a detailed discussion of the development risks defence and its impact on innovation, see Fondazione Rosselli 2004.
3.2.1.7. Relation with regulation

The PLD does not deal extensively with the relation between product regulatory regimes and product liability. It is generally recognized, however, that failure of product to comply with mandatory regulatory standards renders a product defective; the producer is liable for damage if it was caused by the defect.

The converse is also true: the PLD exonerates the producer from liability if it proves that the defect is due to compliance “with mandatory regulations.” It is not sufficient that the product complies with regulations, such as regulations imposing minimum safety and/or efficacy requirements; the producer must also prove that regulation, directly or indirectly, required that the defect be present in the product.

Compliance with any regulatory or voluntary standards that may apply to security products, does not shield the producer from liability under the PLD. This is the case only if the defect is caused by such compliance or is its inevitable result.94

National courts may take compliance with product regulations or standards into account to determine whether a product is defective or meets the state of the art, which may constitute a separate defence. This is, however, left to national courts.

3.2.1.8. Financial security and compensation mechanisms

The PLD does not set forth any provisions related to financial security or compensation. Insurance is not required.

3.2.1.9. Rules of evidence

The claimant bears the burden of proof of the defect, the damage and the causal link between the defect and the damage (PLD, Art 4); the producer bears the burden of proof of any available defence (PLD, Art 7). The standard of proof may differ among the EU Member States (see Work Package 2).

Circumstances specific to security products may complicate the gathering of evidence. A terrorist attack may destroy any proof available and investigations by authorities (and related confidentiality concerns) may hinder the collection of evidence by private parties. Further, security products are typically used by people and it may be difficult to distinguish defects in products from inadequate services.

3.2.1.10. Jurisdictional and procedural issues

The PLD provides that any claim is barred after a period of 3 years starting on the day the plaintiff “became aware, or should reasonably have become aware,” of the three elements of the claim, namely the defect, the damage and the identity of the producer (PLD, Art 10). No claim is admissible after 10 years have lapsed since the producer put the product into circulation (PLD, Art 11).

The PLD does not address jurisdictional and procedural issues.

94 Hodges 1993, p. 75.
3.2.1.11. Applicability in time

The PLD had to be transposed into national law by 1988. It expressly excludes retroactive application of its liability regime to products put into circulation before the deadline for transposition (PLD, Art 17).

3.2.1.12. Conclusions Product Liability Directive

At the EU level, the PLD regime is a critical liability regime for security products, but it does not cover security services. It imposes strict liability on producers for defective products. A product is defective if it does not meet the safety expectations of the public-at-large.

The PLD may create specific challenges for the security industry. Some security products are intended to protect against risks intentionally created by terrorists, who are trying to circumvent or 'outsmart' security systems in an attempt to cause massive damages. The concept of design defect raises issues: the design of security product could be deemed defective if it did not protect against a specific risk, even if this risk is not detectable. Whether a security product’s design is defective is a function of the public’s expectations. Security product providers are not in a position to influence the expectations of the public-at-large, because they have limited access to the public and information on the limitations of security products cannot be freely circulated for security reasons.

From a law and economics perspective, the specific situation of the security industry may hinder the realization of the objectives of the PLD, i.e. ensuring that products meet expectations. The fact that the PLD regime does not provide a mandatory financial cap does not help much to limit the problem. Likewise, the availability of the development risk (state of the art) defence against known but undetectable risks is not available (or uncertain) in all jurisdictions. Thus, the PLD risks are channelled to the producer of the security product, which may not have effective options to address this risk.

There are ways in which these issues could be addressed under the PLD. The PLD could provide, for instance, that security products complying with European or national standards are presumed to be non-defective. Such a link to standards would resolve issues over the putative defectiveness of security products.

3.2.2. General Product Safety Directive 2001/95

3.2.2.1. Brief summary of the regime

The GPSD requires that producers and distributors place only safe products on the market. Products that are produced according to certain standards, as described below, benefit from a presumption of safety. Once the product is placed on the market, producers and distributors must take measures to enable themselves to be informed of risks and take appropriate action to avoid the risks, including through traceability of products, withdrawal from the market, warning consumers, recalling the product from consumers and informing the authorities. Member States are responsible for market surveillance and for imposing effective, proportionate and persuasive penalties applicable to infringements.
3.2.2.2. Key Objectives

The purpose of the GPSD is to protect consumers by requiring producers to place only safe products on the market.

3.2.2.3. Key Instruments

(i) Design requirement
Producers must ensure that products placed on the market are safe. Distributors have a duty of care to consumers, including an obligation not to place products on the market if they know or should have known that these products are unsafe.

Under the GPSD, a ‘safe product’ means ‘any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons’ (GPSD, Article 2(b)). This definition does not include the ‘absence of a claimed positive effect,’ for example, a battery that does not last as long as it should have, unless this absence is characterized as a risk.

Elements that are taken into account when determining whether a product is safe include: (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance; (ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products; (iii) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product; and (iv) the categories of consumers at risk when using the product.

The availability of product design features that increase safety is irrelevant to determine whether a product is safe.

Products that conform to approved European standards or to EU or national safety rules are presumed safe.\(^95\) If no such standards or rules are in place, the conformity of a product to the general safety requirement shall be assessed based on following elements:

- voluntary national standards (transposing relevant European standards not published in the Official Journal);
- national standards;
- Commission guidelines;
- product safety codes of good practice of the relevant sector;
- the state of the art and technology; and
- reasonable consumer expectations concerning safety.

Conformity with any rule or standard does not prohibit, however, that Member States take measures, including product recall, if a compliant product is dangerous.

\(^{95}\) In a Commission report on the implementation of Directive 2001/95/EC that was released on 14 January 2009, COM (2008) 905, the Commission pleads for a simplification of the standardisation provisions to allow for a greater flexibility.
A security product could be deemed unsafe, if it causes harm to individuals in the course of its normal use, e.g., by radiation. Some security products may be subject to standards that offer criteria to determine whether a product is safe.

Several RAPEX notifications have been submitted on alarm products that are deemed insufficiently sensitive. These notifications are made to the European Commission by Member States for products posing a serious risk through the EU Rapid Information System (RAPEX). This suggests that security products that are inherently safe, but are not sensitive enough to detect the risk they are designed to address, may also be held unsafe. The definition of “safe product,” including the standard that a product do not “present any risk,” is apparently construed by the Member States to include both positive risks (capacity to cause harm) and negative risks (capacity to prevent harm caused by persons or other products). It would be far-fetched to argue that passengers, following a terrorist attack, could successfully claim that the security equipment concerned was not safe under the definition of “safe product” as set out in the GPSD, because the issue is the absence of a positive effect on security in general, i.e., detection of a risk posed by another passenger.

(ii) Traceability and post-marketing monitoring requirements
Producers and distributors must ensure the traceability and monitor the safety of products on the market, for example by testing samples and keeping a register of complaints.

(iii) Informational, reporting, and disclosure requirements vis-à-vis government agencies and/or consumers
Producers must provide consumers with the relevant information to enable them to assess the risks inherent in a product throughout the normal period of its use, especially when those risks are not obvious. This must allow consumers to take adequate precautions.

Producers and distributors must immediately report any unsafe product on the market to the competent authorities in the Member States.

(iv) Corrective measures
If products placed on the market are unsafe, producers must take appropriate corrective actions, including informing consumers, up to product recall, as a last resort. In these cases, producers and distributors must also notify the authorities (see above), and cooperate with them.

3.2.2.4. Regulated entities, activities and products

The GPSD imposes requirements on both producers and distributors. A producer is defined as the manufacturer or the company that brands the product and any professional in the supply chain whose activity may affect the safety properties of a product. In the case of imports, the producer is deemed to be the manufacturer’s EU representative or, in the absence of a representative, the importer.

Distributor is defined as “any professional in the supply chain whose activity does not affect the safety properties of a product” (GPSD, Article 2(f)).

The GPSD covers all products that are “intended for consumers or that are likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them,”
and are “supplied or made available, whether for consideration or not, in the course of a commercial activity (GPSD, Article 2(a)).”  

The notion of ‘consumers’ is not defined in the GPSD. Most EU directives define a consumer as “a natural person who, is acting for purposes which are outside of his trade, business or profession.”  

The GPSD is also applicable to products provided in relation with a service and is applicable regardless of whether the products are new, used or reconditioned. The GPSD does not apply, however, to second-hand products supplied as antiques or as products to be repaired or reconditioned prior to being used, provided that the supplier clearly informs the customer to that effect.  

Most security products would appear to fall outside the GPSD’s scope, since they are generally not intended for consumers. Certain security products such as alarm systems or bullet proof vests, however, could be used by individuals in a non-professional capacity and thus fall under the GPSD. A scanner in an airport is “used” on (and for the protection of) consumers (i.e., the passengers in an airport), but not “by” consumers and would thus fall outside the scope of the GPSD.  

The GPSD set forth requirements for producers, distributors and Member States. The obligations imposed on producers are discussed under 2 and 3, above.  

3.2.2.5. Relation with liability  

The GPSD is not a liability programme but potentially affects liability exposure in opposite ways. On one hand, it can expand liability exposure where:  

(i) it increases the applicable standards by requiring all consumer products to be placed on the market to present no risks or only the minimum risks compatible with the product’s use, considered to be acceptable and consistent with a high level of protection for the health and safety of persons;  

(ii) it requires disclosure of information on the basis of which claims could be asserted. Specifically, producers and distributors are required to inform the authorities of any product that could be dangerous. This opens the door to claims by individual consumers of these goods.  

(iii) non-compliance with the regulatory standards constitutes breach of obligation or negligence per se, which may trigger liability exposure. If a product does not meet the GPSD’s safety requirements, its producer and/or distributor is exposed to fines. This, in turn, may constitute an argument to support a claim that the producer and/or distributor is liable under civil law for damage caused by the unsafe product. Non-compliance with the post-marketing requirements of the GPSD may also be construed as negligence, which may trigger liability exposure. For example, if a producer negligently does not take any corrective measure against an unsafe product, it may be held liable for material damages under the Product Liability Directive, but also for economic damages based on tort law, if the claimant proves that there is a link between the negligence and his or her damage.  

On the other hand, compliance with the GPSD could potentially limit effective liability exposure if:

(i) companies adopt measures to avoid that unsafe products are being placed on the market, or, if they are placed on the market, to mitigate any adverse consequences;

(ii) a product that is “safe” under the GPSD may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with the regulatory standards does not preclude potential civil liability exposure; for example, the PLD does not provide for this, so it will not be a decisive factor.

3.2.2.6. Financial security and compensation mechanisms

The GPSD does not set forth any provisions related to financial security or compensation or compensation. Insurance is not required.

3.2.2.7. Applicability in time

The GPSD repeals Directive 92/59/EEC. All references to the aforementioned Directive shall be construed as reference to the GPSD and read in accordance with the correlation table.

Member States had to transpose the GPSD by 15 January 2004.

The GPSD does not set forth any transitional measures that may have an impact on liability, such as grandfathering provisions.

3.2.2.8. Other relevant features

(i) Market surveillance and European cooperation

The GPSD requires that Member States appoint a competent authority that is responsible for market surveillance and has the power to impose penalties on producers and distributors that do not comply with the national provisions adopted pursuant to the GPSD. Member States must actively identify products posing a serious risk to health and safety by organizing appropriate checks before and after any product is placed on the market. If they find products posing serious risks, they must take rapid measures of intervention to protect consumers, and immediately inform the Commission via the RAPEX system. This system is meant to exchange information between the Commission and the Member States quickly, thereby enabling distribution of dangerous products to be limited or prevented.

Under the RAPEX system, Member States must provide the Commission with at least the following information:

- information enabling the product to be identified;
- a description of the risk inherent in the product, as well as any documents enabling its assessment;
- details of measures already taken;

An inventory was made in 2004 setting out the detailed provisions of GPSD and the relevant corresponding national transposition measures, <http://ec.europa.eu/consumers/cons_safe/keydocs/gpsd_comp_inv_a_en.pdf>, accessed 1 December 2012.
- information on distribution of the product.\textsuperscript{99}

(ii) European emergency measures

If the Commission is aware that a specific product poses a serious risk to the health and safety of consumers in various Member States, it can also implement measures, such as ban, product recall or warning label, at a European level. After consultation with the Member States, the Commission can adopt decisions with a maximum duration of 1 year, which can be extended for additional periods of maximum 1 year (GPSD, Article 13(2)).

The Commission may adopt a measure if (i) the Member States adopt diverging approaches to dealing with the risks posed by such dangerous products; (ii) urgency is required due to the risk posed by the product and no other Community laws deal with that risk; and (iii) such measure is the most effective way of eliminating the risk.

The Commission has taken four emergency decisions so far; they were related to phthalates, lighters, magnetic toys and dimethylfumarate.\textsuperscript{100}

3.2.2.9. Conclusions Product Safety Directive and Implications for Security Industry

The GPSD affects a limited number of security products, namely those that are intended for or may be used by consumers. Note, however, that specific rules with similar aims to the ones of the GPSD apply to products covered by EU harmonization legislation, and also other products.\textsuperscript{101}

Under the GPSD, product safety is determined with reference to standards and rules. If security products are covered by such instruments, compliance implies safety and thus offers legal certainty to the security industry. This legal certainty is limited to administrative law, however, and does not protect against civil liability exposure.

Further, the GPSD requires the necessary measures to prevent or mitigate any damage from all actors in the supply chain, not only from the manufacturer of the security product. By imposing reporting requirements for unsafe products on the market, and certain other features, however, the GPSD might \textit{de facto} increase the civil liability exposure of the security industry.

3.2.3. REACH Regulation 1907/2006 and CLP Regulation 1272/2008

3.2.3.1. Brief summary of the regime

The REACH Regulation\textsuperscript{102} and the CLP Regulation\textsuperscript{103} provide a comprehensive regulatory regime to regulate chemicals. These regulations require chemical companies and, to lesser

\textsuperscript{99} In 2004, a specific guidance was released to ensure the efficient operation of RAPEX, Commission Decision 2004/418/EC.


\textsuperscript{101} Regulation (EC) 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) 339/93 [2008] OJ L 218/30, Articles 15 and following.

extent, product companies, to assess the hazards of their chemicals and products, how to safely use them, to communicate this information to customers and to safely use chemicals and products. They also entitle authorities to adopt additional regulations, including bans and information requirements.

3.2.3.2. **Key Objectives**

The main purposes of the REACH Regulation are to “ensure a high level of protection of human health and the environment as well as the free movement of substances, on their own, in mixtures and in articles, while enhancing competitiveness and innovation.” The CLP Regulation has similar purposes.

3.2.3.3. **Key Instruments**

The REACH Regulation and the CLP Regulation set forth a particularly comprehensive regulatory program to address the risks created by chemicals, including registration, notification, communication requirements, authorization and restriction. We review the rules relevant to the purposes of this Study.

(i) registration, notification, or authorization requirements

**Notification requirement under the CLP Regulation.** The CLP Regulation requires suppliers of substances and mixtures to classify and label their chemicals (see below) based on their physico-chemical, toxicological and eco-toxicological hazards. Suppliers are responsible to classify and label their substances based on the criteria set forth under the CLP Regulation, unless the CLP Regulation itself impose an harmonized classification or labelling on a particular substance (CLP, Annex VI). They must also notify this classification and labelling to ECHA (CLP, Art 40). Contrary to the REACH Regulation (see below), suppliers are not required to test to generate new data, unless for physicochemical properties.

**Registration requirement under the REACH Regulation.** The REACH Regulation is based on the principle “no data, no market” (REACH, Art 5). No chemical substance must be manufactured or imported unless it has been registered with the European Chemicals Agency (ECHA) (REACH, Arts 6, 7, 10, 12, 13, 14, 17 and 18). This requirement extends to substances in mixtures, such as paints, and in articles, if there is an intended release of that substance from the article. Registrants must submit information on their substances, including physico-chemical, toxicological, eco-toxicological and Persistent, Bioaccumulative and Toxic/very Persistent very Bioaccumulative (PBT/vPvB) information as well as classification and labelling in accordance with the CLP Regulation 1272/2008. Depending on the tonnage band, registrants must provide information on certain endpoints, either by testing in accordance with the Test Methods Regulation\(^\text{104}\) or by a valid alternative method (REACH, Art 13, Annexes VI-X, column 2 and Annexes XI), such as read-across.

If the substance is hazardous and manufactured or imported above 10 tonnes per year, the registrant must also develop so-called “exposure scenarios” describing how the substance can safely be used (REACH, Art 14 and Annex I).


Notification to obtain an exemption from registration for research and development projects under the REACH Regulation. REACH provides that companies may obtain a time-limited exemption from registration for product and process orientated research and development by notifying some limited information, including estimated quantity and list of customers, to ECHA (REACH, Art 9). ECHA may impose certain restrictions to the use of notified substances.

Notification for substances in articles under the REACH Regulation. REACH entitles ECHA to add substances of very high concern on a Candidate List. These substances are carcinogenic, mutagenic or toxic to reproduction substances (CMR), persistent, bioaccumulative and toxic (PBT), very persistent and very bioaccumulative (vPvB) substances and substances of “equivalent concern,” such as endocrine disrupters (REACH, Art 57).

If a listed substance is present in articles above 0.1% per weight and 1 tonne per year, the supplier of the article must also notify certain information to ECHA (REACH, Art 7(2)). This information includes the classification of the substance in accordance with the CLP Regulation, use information and the tonnage band.

Authorization under the REACH Regulation. Under certain conditions, all uses of certain substances, including manufacture and incorporation into articles, may be subject to authorization by the European Commission (REACH, Arts 55 to 66). The authorization may only be granted if either the applicant can establish that the substance may be safely used – i.e., the risks to human health or the environment are adequately controlled during the life-cycle of the substance - or socio-economic benefits of using the substance outweigh the risks and there is no suitable alternative (REACH, Arts 60(3) and (4)). The authorization may impose any condition on the use of the substance, such as monitoring, (REACH, Art 60(8)) and must be reviewed within a period of time to be set by the authorization (REACH, Art 60(8)). Regardless of the review period, the authorization may be withdrawn in certain cases (REACH, Art 61(2)), including if new information possible alternatives become available.

(ii) Use or design requirements (means and/or results requirements)

General use requirements under the REACH Regulation. If exposure scenarios are developed (see above), these are communicated within the suppliers and both registrants and users must comply with them (REACH, Arts 14(6) and 37(5)). These exposure scenarios may contain occupational conditions and risk management measures, such as ventilation and protective glasses, to safely use substances. Use requirements may be more stringent (“strictly controlled conditions”) if the substance is registered as intermediate, which requires to submit less information than registration as a full substance (REACH, Arts 17 and 18).

Specific use requirements under the REACH Regulation. ECHA and the European authorities may impose certain conditions for substances notified for process orientated research and development (PPORD) use or subject to authorization (see above).

Restrictions under the REACH Regulation. The REACH Regulation establishes a list of restriction on the use of chemicals on their own, in mixtures and articles (REACH, Annex XVII). For example, nickel is prohibited in articles intended to come into direct and prolonged contact with the skin (REACH, Annex XVII, entry 27).

Packaging requirement under the CLP Regulation. The CLP Regulation imposes certain packaging requirements (CLP, Article 35), including childproof fastener, on hazardous chemicals.
(iii) informational, reporting, and disclosure requirements vis-à-vis government and/or customers and consumers

The CLP Regulation provides that Member States must appoint a body responsible to receive from chemical companies information related to their chemicals in order to prepare preventative and curative measures, in particular in the case of emergency health response (CLP, Art 45).

The REACH and CLP Regulations require chemicals companies to label their chemicals with hazard information (CLP, Arts 17-33) and to communicate to their customers and consumers a guide on the safe use of their substances (REACH, Arts 31-32; for consumers, see REACH, Art 31(4)).

All workers are entitled to this guidance on safe use of chemicals that they use or may be exposed to in the workplace (REACH, Art 35).

Article suppliers must also automatically provide to their customers information on how to safely use their articles, if they contain a substance on the Candidate List above 0,1% weight by weight. This information must, at least, contain the name of that substance (REACH, Art 33(1)). Similar information must be provided to consumers upon request (REACH, Art 33(2)).

(iv) post-marketing monitoring requirements and related reporting obligations

If there is new information on chemical hazards or risks, registrants must update their registration dossier and guide on the safe use of substance (REACH, Arts 22, 31(9) and 32(3)). This updating requirement may be viewed as implicitly requiring registrants to actively monitor new developments related to their substances.

Suppliers of chemicals must also update their classification and labelling under the CLP Regulation, which expressly requires these companies to “take all reasonable steps” to make themselves aware of new scientific or technical information (CLP, Arts 15 and 30).

In addition, the REACH Regulation requires professional actors within the supply chain to communicate to their suppliers any new information on chemical hazards and risks (REACH, Art 34).

3.2.3.4. Regulated entities, activities and products

The REACH Regulation applies to all chemical entities, including manufacturers, importers, distributors and professional users. It also imposes obligations on suppliers of products.

The CLP Regulation applies to all chemical entities.

3.2.3.5. Relation with liability

Neither the REACH Regulation nor the CLP Regulation set forth any civil liability rules but each of them can potentially affect civil liability exposure in opposite ways. On one hand, either of these regimes can expand liability exposure where:

- it raises the applicable standards by requiring all chemicals and products to be placed on the market to conform to certain requirements, including ‘safe use’ requirements.
- it requires disclosure of information on the basis of which claims could be asserted. This opens the door to claims by individual companies and consumers regarding these products.
- non-compliance with the standards constitutes breach of obligation or negligence per se, which may trigger liability exposure.

On the other hand, compliance with these regulations could potentially limit effective liability exposure because:

- companies must research the hazard of their chemicals and adopt measures to ensure safe use of chemicals and products, which may result in fewer accidents;
- a product that is “safe” or is accompanied by the necessary information to be “safely used” under the REACH and CLP Regulations may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with the regulatory standards does not preclude potential civil liability exposure; the PLD does not provide for this, so it will not be a decisive factor.

3.2.3.6. Financial security and compensation mechanisms

Neither the REACH Regulation nor the CLP Regulation set forth any provisions related to financial security or compensation or compensation. Insurance is not required.

3.2.3.7. Application in time

The REACH and CLP Regulations entered into force on 1 June 2007 and 20 January 2009, respectively. These Regulations brought enormous changes to European chemical law and, therefore, provided for a gradual effective date of its various requirements.

For example, the registration requirement became effective from 1 June 2008. However, because such requirement imposed significant preparation from industry on most substances already on the market at that time, the REACH Regulation provided a phase-in regime. Provided that the substance is pre-registered with ECHA, which requires minimum information, manufacturers and importers are only required to register by:

- 1 December 2010: substances that are (1) classified as carcinogenic, mutagenic or toxic to reproduction and manufactured or imported in quantities reaching one tonne per year, (2) substances classified as very toxic to aquatic organisms which may cause long-term adverse effects in the aquatic environment and manufactured or imported in quantities reaching 100 tonnes per year, and (3) manufactured or imported in quantities reaching 1,000 tonnes per year.
- 1 June 2013: substances manufactured or imported in quantities reaching 100 tonnes per year.
- 1 June 2018: substances manufactured or imported in quantities reaching 1 tonne per year.

Implementing measures, such as inclusion of substances on the Candidate List or the Authorization List, may also be subject to transitional measures. For example, the obligation to notify ECHA regarding substances in articles, only applies 6 months after that substance is added to the Candidate List (REACH, Art 7(7)). Further, any decision to add a substance to the Authorization List must set forth transitional arrangements (REACH, Art 58(1)(c)).
3.2.3.8. Other relevant features

(i) Data sharing
In order to avoid unnecessary animal testing and to reduce costs for the industry, the REACH Regulation requires potential registrants and registrants of the same substance to share data (and related costs) required for registration or, where new information must be generated, to conduct a single test (REACH, Arts 11, 19, 26-30, 40(3)(e) and 53).

(ii) Enforcement
Member States are responsible to enforce the REACH and CLP Regulations and to adopt “effective, proportionate and dissuasive” sanctions (CLP, Arts 46 and 47, and REACH, Arts 125 and 126).

ECHA must also assess at least 5% of all registration dossiers for compliance with the REACH Regulation and requires registrants to update their dossier in the case of noncompliance (REACH, Art 41).

3.2.3.9. Conclusions REACH and implications for security industry

The REACH and CLP Regulations provide comprehensive regulatory programs for addressing all risks for human health and the environment created by substances throughout their lifecycle. They require detailed hazard and safety information prior to the substance being placed on the market, and communication of this information within the supply chain and to consumers, and provide for command-and-control options for the authorities if they deem the measures taken by industry to be insufficient.

Security products are articles, not substances or mixtures, under REACH, and thus are affected only by REACH’s substances in articles regime. Both regulations are intended to address risks to human health and the environment, but not other security risks. These regulations are thus of little direct relevance for this study. They may potentially be relevant, however, if hazardous substances that are critical to the security industry are regulated under the REACH authorization program. The aviation industry already experienced this issue.105

The emphasis on disclosure of information on products, costs, and limited incentives for innovation created by these regulations106 make them unsuitable as a regulatory model for the security industry. Most features of these regulatory programs could hardly be applied to the security industry, or are not relevant to security products. Disclosure of information on security products could even be positively harmful.

---

3.2.4. **Plant Protection Product Regulation 1107/2009**

3.2.4.1. *Brief summary of the regime*

The Plant Protection Product Regulation\(^{107}\) (PPPR) harmonizes rules on effectiveness and safety of plant protection products, such as pesticides. This regulation requires authorization to place PPP on the market and market surveillance.

3.2.4.2. *Key Objectives*

The main purpose of the PPPR is to harmonize the rules on the placing of PPP on the market and to ensure a high level of health and environmental protection.

3.2.4.3. *Key Instruments*

All active substances in PPP must be assessed and approved at the European level. Criteria for authorization include efficacy of the substance and its impact on human health and the environment.

The placing on the market of all PPP is further subject to authorization to be granted by Member States.

The authorisation must include requirements on the placing on the market of the PPP and conditions of use (PPPR, Art 31), which could include an obligation to inform neighbours who could be exposed to PPP before using it and obligation to provide a label and indications for proper use of the PPP.

The PPPR also regulates the advertising of PPP and requires, a.o., that all statements in advertising be technically justifiable (PPPR, Art 66).

3.2.4.4. *Regulated entities, activities and products*

PPP are defined as “products, in the form in which they are supplied to the user, consisting of or containing active substances, safeners or synergists, and intended for one of the following uses:

(a) protecting plants or plant products against all harmful organisms or preventing the action of such organisms, unless the main purpose of these products is considered to be for reasons of hygiene rather than for the protection of plants or plant products;
(b) influencing the life processes of plants, such as substances influencing their growth, other than as a nutrient;
(c) preserving plant products, in so far as such substances or products are not subject to special Community provisions on preservatives;
(d) destroying undesired plants or parts of plants, except algae unless the products are applied on soil or water to protect plants;
(e) checking or preventing undesired growth of plants, except algae unless the products are applied on soil or water to protect plants.” (PPPR, Art 2(1))

Regulated entities are producers of PPP, defined as “a person who manufactures plant protection products, active substances, safeners, synergists, co-formulants or adjuvants on his own, or who contracts this manufacturing to another party, or a person designated by the manufacturer as his sole representative for the purpose of compliance with this Regulation” (PPPR, Art 3(11)).

Professional users are also subject to certain requirements, such as the obligation to keep records of the PPP they use during at least 3 years (PPPR, Art 67).

3.2.4.5. Relation with liability

The PPPR is not a liability programme but it potentially affects liability exposure in opposite ways. On one hand, it can expand liability exposure where:

- it raises the applicable standards by requiring all PPP to conform to certain restrictions. It may also require certain conditions on the use of PPP.
- it requires disclosure of information on the basis of which claims could be asserted. This opens the door to claims by individual consumers regarding these goods.
- non-compliance with the standards constitutes breach of obligation or negligence per se, which may trigger liability exposure.

On the other hand, compliance with this regulation could potentially limit effective liability exposure because:

- companies must research the hazard of their products and adopt measures to ensure safe use of PPP, which may prevent accidents;
- a product that is “safe” or is accompanied with the necessary information to be “safely used” under the PPPR may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with regulatory standards does not preclude potential civil liability exposure (PPPR, Art 73); the PLD does not provide for this, so it will not be a decisive factor.

3.2.4.6. Financial security and compensation mechanisms

The PPPR does not set forth any provisions related to financial security or compensation or compensation. Insurance is not required.

3.2.4.7. Application in time

The PPPR entered into force on 14 December 2009 and became effective on 14 June 2011. It repeals the Directive 91/414/EEC that nevertheless continues to apply to certain active substances (PPPR, Art 80). Products labelled in accordance with Directive 91/414/EEC may also continue to be placed on the market until 14 June 2015 (PPPR, Art 80(6)).

Member States may also adopt certain temporary derogations for safeners, synergists, co-formulants and adjuvants (PPPR, Art 81).

3.2.4.8. Other relevant features

Member States are responsible to enforce the PPPR and must adopt “effective, proportionate and dissuasive” sanctions (PPPR, Art 72).
3.2.4.9. Conclusions Plant Protection Product Regulation and implications for security industry

The PPPR provide a comprehensive regulatory program to address all risks for human health and the environment created by PPP. It requires detailed hazard and safety information prior to the substance being placed on the market, and communication of this information within the supply chain. It also allows for the possibility to adopt use requirements.

The PPPR does not apply to security products and is intended to address risks to human health and the environment, but not terrorism risks. This regulation is thus of little direct relevance for this Study.

3.2.5. EUDRALEX

3.2.5.1. Brief summary of the regime

European law harmonizes the rules on effectiveness and safety of medicinal products. It requires authorization of medicinal products before they can be placed on the market and authorization is dependent on showing that the medicinal product is both safe and effective. It also requires to provide information to patients and manufacturing and post-marketing obligations.

EUDRALEX is a compilation of European laws and guidelines applicable to medicinal products. For the purpose of this Study, we focus on the main piece of legislation relevant to medicinal products for human use, Directive 2001/83/EC on the human medicinal code (“Medicinal Code”).

3.2.5.2. Key Objectives

The purpose of the Medicinal Code is to harmonize the rules on the placing of medicinal product on the market and to safeguard public health (Medicinal Code, recital 3).

3.2.5.3. Key Instruments

(i) registration, notification, or authorization requirements
The efficacy and safety of medicinal products must be assessed and their placing on the market is subject to authorization (Medicinal Code, Arts 6 and following). Manufacturers of medicinal products are also subject to authorization and must comply with good manufacturing practices (Medicinal Code, Arts 40 and following). Wholesalers are also subject to authorization and comply with good distribution practices (Medicinal Code, Arts 76 and following).

(ii) Design and use requirements (means and/or results requirements)
Authorization for a medicinal product must be rejected if the product is harmful in normal conditions of use, its therapeutic efficacy is lacking or insufficiently substantiated or its qualitative and quantitative composition is not declared (Medicinal Code, Art 26).

Their use may also be subject to restriction, such as medical prescription (Medicinal Code, Art 70).

(iii) informational, reporting, and disclosure requirements vis-à-vis government and/or customers and consumers
Medicinal Products must be labelled and have a package leaflet to ensure its safe use (Medicinal Code, Arts 54 and following). The advertising of medicinal products is also severely restricted (Medicinal Code, Arts 86 and following).

(iv) post-marketing monitoring requirements and related reporting obligations
Marketing authorization holders must conduct pharmacovigilance activities and regularly report on these activities to the competent authority (Medicinal Code, Arts 101 and following). They must also regularly assess information available on their products and, where relevant, generate further information. A marketing authorization may also be subject to certain obligations, such as carrying out further post-marketing testing (Medicinal Code, Art 22).

3.2.5.4. Regulated entities, activities and products

The Medicinal Code covers industrial medicinal products, defined as “(a) [a]ny substance or combination of substances presented as having properties for treating or preventing disease in human beings; or (b) [a]ny substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis.” (Medicinal Code, Art 1(2)).

Regulated entities are marketing authorization holders, importers, manufacturers of medicinal products and ingredients and distributors.

3.2.5.5. Relation with liability

The Medicinal Code provides that, without prejudice to the PLD, regulated entities must not be subject to civil or administrative liability for unapproved use of medicinal products, if such use is recommended or required by the authorities in response of suspected or confirmed spread of harmful products, such as toxins or nuclear radiation (Medicinal Code, Arts 5(3) and (4)).

The Clinical Trials Directive 2001/20/EC provides that a clinical trial may be conducted only if the liability of the investigator and sponsor is covered by an insurance or an indemnity (Clinical Trials Directive, Art 3(2)(f)). This Directive is currently under review and could in the future remove this requirement for low-risk trials and require Member States to set up a national indemnification mechanism. 109

Otherwise, the Medicinal Code is not a liability programme but it potentially affects liability exposure in opposite ways. On one hand, it can expand liability exposure where:

109 “This obligatory insurance/indemnity has substantially increased the costs and administrative burden of conducting clinical trials, but there is no evidence that the number of damages, or the amount, has increased with the entry into force of the Directive.” European Commission, “Proposal for a Regulation of the European Parliament and of the Council on Clinical Trials on Medicinal Products for Human Use, and Repealing Directive 2001/20/EC” COM(2012) 369, 9.
- it raises the applicable standards applicable to all medicinal products.
- it requires disclosure of information on the basis of which claims could be asserted. This opens the door to claims by individual consumers regarding these goods.
- non-compliance with the standards constitutes breach of obligation or negligence per se, which may trigger liability exposure.

On the other hand, compliance with this regulation could potentially limit effective liability exposure because:

- companies must assess and monitor the efficacy and safety of their products;
- a product that is “safe” or is accompanied with the necessary information to be “safely used” under the Medicinal Code may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with the regulatory standards does not preclude potential civil liability exposure (Medicinal Code, Arts 25 and 61(4)); the PLD does not provide for this, so it will not be a decisive factor.

3.2.5.6. Financial security and compensation mechanisms

The Medicinal Code does not set forth any provisions related to financial security or compensation or compensation. Insurance is not required.

3.2.5.7. Application in time


3.2.5.8. Other relevant features

Member States are responsible to enforce the Medicinal Code and must adopt “effective, proportionate and dissuasive” sanctions (Medicinal Code, Arts 111-119).

3.2.5.9. Conclusions EUDRALEX and implications for security industry

The Medicinal Code provides a comprehensive regulatory program to regulate medicinal products for human use. It requires detailed information prior to the product being placed on the market, authorization of products and manufacturers, communication of product information within the supply chain and post-marketing surveillance.

The Medicinal Code does not apply to security products and is not intended to address terrorism risks. This legislation is thus of little direct relevance for this Study. It does set forth a specific feature, however, that is relevant, by analogy to the security industry: companies must not be subject to civil or administrative liability for unapproved use of medicinal products, if such use is recommended or required by the authorities to address a suspected or confirmed public health problem.

3.2.6.1. Brief summary of the regime

The Council Directive of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment (“PPE Directive” or “Directive”) lays down the conditions governing the placing on the market and free movement within the EU of personal protective equipment (“PPE”) and the basic safety requirements which must be met to ensure the health protection and safety of users. The PPE Directive defines only the basic requirements to be satisfied by personal protective equipment. Harmonized European standards have been developed in order to facilitate proof of conformity with those basic requirements. Compliance with these standards confers a presumption of conformity on the PPE and the producers.

3.2.6.2. Key Objectives

The objective of the PPE Directive is to ensure the free movements of PPE in Europe.

3.2.6.3. Key Instruments

Member States must take all appropriate measures to ensure that the PPE that are covered by the Directive may only be placed on the market and brought into service when, if properly maintained and used for its intended purpose, it preserves the health and ensures the safety of users without prejudice to the health or safety of other individuals, domestic animals or goods (PPE Directive, Art 3). All PPE must satisfy the basic health and safety requirements as set out in Annex II (PPE Directive, Art 3).

Manufacturers must follow a certification procedure managed by a notified body before PPE can be placed on the market:

- If the product is of simple design where it can be assumed that the user can assess the provided protection level himself, no EC type-examination is required. These products of simple design cover only PPE that is meant to protect the user against smaller risks and include products such as gardening gloves, seasonal clothing and sunglasses. (PPE Directive, Art 8.3)
- If PPE is of complex design, EC type-examination is required prior to the series production of the product (PPE Directive, Art 8.2). Additionally, production of PPE is subject to one of the following procedures (1) EC quality control for the final product; or (2) quality control system for the production process.

3.2.6.4. Regulated entities and activities or products

(i) Regulated products and activities
PPE is defined as “any device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards” (PPE Directive, Art 1.2).

PPE shall also cover:

“(a) a unit constituted by several devices or appliances which have been integrally combined by the manufacturer for the protection of an individual against one or more potentially simultaneous risks;
(b) a protective device or appliance combined, separable or inseparably, with personal
non-protective equipment worn or held by an individual for the execution of a specific
activity;
(c) interchangeable PPE components which are essential to its satisfactory functioning
and used exclusively for such equipment.” (PPE Directive, Art 1.2)

PPE covered by other directives with similar goals and PPE mentioned in the exhaustive list
in Annex I are exempt from the PPE Directive. Annex I includes the following exemptions
relevant to the security industry: (i) PPE to be used by armed forces or in the maintenance of
public order such as helmets and shields; (ii) PPE for self-defence such as personal deterrent
weapons; and (iii) PPE intended for the protection or rescue of persons on vessels or aircraft,
not worn all the time.

Most PPE used by the security industry, such as shields, are thus excluded from the scope of
the PPE Directive. Other PPE, such as protective gloves, are used by various industries, not
specifically by the security industry with the intent to reduce the risks of intentional damage
caused by terrorism and organized crime, and thus are not security products.

(ii) Regulated entities
Regulated entities are manufacturers of PPE.

3.2.6.5. Relation with liability

The PPE Directive is not a liability programme but potentially affects liability exposure in
opposite ways. On one hand, it can expand liability exposure where:

(i) it raises the applicable standards by requiring all PPE to be placed on the market to
present no risks or only the minimum risks compatible with the product’s use,
considered to be acceptable and consistent with a high level of protection for the
health and safety of persons;

(ii) non-compliance with the regulatory standards constitutes breach of obligation or
negligence per se, which may trigger liability exposure. If a product does not meet the
PPE Directive’s safety requirements, its producer and/or distributor is exposed to
fines. This, in turn, may constitute an argument to support a claim that the producer is
liable under civil for damage caused by the unsafe product.

On the other hand, compliance with the PPE Directive could potentially limit effective
liability exposure if:

(i) companies adopt measures to avoid that unsafe PPE are being placed on the market;

(ii) a product that is “safe” under the PPE Directive may de facto be regarded as not being
“defective” under the PLD. Note, however, that compliance with the regulatory
standards does not preclude potential civil liability exposure; the PLD does not
provide for this, so it will not be a decisive factor.

3.2.6.6. Financial security and compensation mechanisms

The PPE Directive does not provide for any mechanisms of financial security or
compensation for producers. The PPE Directive, however, requires notified bodies to have an
insurance covering their civil liability, unless that liability is covered by the Member State
3.2.6.7. Applicability in time

The PPE Directive was amended several times and for the last time in 2003. It had to be transposed before December 31, 1991 and Member States were required to apply its measures as of July 1, 1992. It provides for a phase-in regime where Member States had to allow the placing on the market and putting into service of PPE in conformity with the national regulations in force in their respective territory on 30 June 1992, until 30 June 1995 (PPE Directive, Art 16). The EU-25 have all implemented the Directive.\textsuperscript{110}

The PPE Directive is currently subject to a revision process. So far, two studies have been ordered and published by the European Commission DG Enterprise and Industry.\textsuperscript{111}

3.2.6.8. Other relevant features

Member States must monitor whether PPE are safe. When PPE that is used in accordance with its intended purpose could compromise the safety of individuals, domestic animals or property, Member States must take measures to remove that equipment from the market and prohibit the marketing or free movement thereof (PPE Directive, Art 7.1). Member States must inform the Commission of any action taken in this regard.

Member States must also check if CE markings are rightfully affixed (PPE Directive, Art 13).

3.2.6.9. Conclusions Personal Protective Equipment Directive and relevance to the security industry

The PPE Directive is a relevant instrument for the purpose of this Study.

Under the regime of the PPE Directive compliance with the applicable European standards automatically confers an assumption of conformity with the basic safety requirements of the PPE. This does not necessarily offer protection against liability to the producers, however; the PLD, for instance, does not provide for any such presumption so it will not be a decisive factor.

PPE are used by the security industry and compliance with the PPE Directive may result in a higher level of safety for users, such as guards. Compliance with the PPE Directive will reduce, but not eliminate, the PPE producer’s liability exposure.

\textsuperscript{110} More details on the national transpositions can be found on the Commission website \url{<http://ec.europa.eu/enterprise/sectors/mechanical/documents/legislation/personal-protective-equipment/transposition/index_en.htm>} accessed 1 December 2012.

3.2.7. Directive 2006/42/EC on Machinery

3.2.7.1. Brief summary of the regime

Directive 2006/42/EC on machinery\textsuperscript{112} (“Machinery Directive”) harmonizes the safety requirements for machinery, using standardization, conformity assessment procedure and CE-marking.

3.2.7.2. Key Objectives

The Machinery Directive aims at ensuring the safe design and construction of machinery and the proper installation of machinery to reduce the social cost of the large number of accidents caused directly by the use of machinery (Machinery Directive, recital 2).

3.2.7.3. Key Instruments

(i) Design requirements

Machinery may only be placed on the market if it does not endanger the health and safety of persons or, where appropriate, domestic animals or property, when properly installed and maintained and used for its intended purpose or under conditions which can reasonably be foreseen (Machinery Directive, Art 4(1)).

These health and safety requirements are set out in Annex I of the Machinery Directive. Compliance must be established via a conformity assessment procedure (Machinery Directive, Art 12). Further, the manufacturer has the “ongoing responsibility of ensuring that the said machinery meets the corresponding state of the art” (Machinery Directive, Annex IX, under 9(2)) if it uses the so-called EC type-examination assessment procedure.

(ii) Informational, reporting, and disclosure requirements vis-à-vis government and/or customers and consumers

Manufacturers are also subject to the following information requirement prior to placing machinery on the market (Machinery Directive, Art 5):

- Make a technical file available,
- Provide all necessary information such as warning or instructions for use (Machinery Directive, Annex I, under 1(7)),
- Assess conformity of machines and draw up an EC declaration of conformity,
- Affix CE marking and ensure the declaration of conformity accompanies the machine.

If these rules are adhered to the machinery is deemed to comply with the provisions of the Machinery Directive.

Machinery that is produced in compliance with a harmonized standard is presumed to comply with the essential health and safety requirements covered by such harmonized standards (Machinery Directive, Art 7(2)).

(iii) post-marketing monitoring requirements and related reporting obligations

If the manufacturer uses the so-called full quality assurance conformity assessment procedure, it must manages a quality system (Machinery Directive, Annex X, under 2(2)), including:

---

- conducting manufacturing, quality control and quality assurance techniques, processes and systematic actions,
- conducting inspections and tests before, during and after manufacture,
- maintaining the quality records, such as inspection reports and test data, calibration data, and reports on the qualifications of the personnel concerned,
- monitoring the achievement of the required design and quality of the machinery, as well as the effective operation of the quality system.

3.2.7.4. Regulated activities or products

The Machinery Directive applies to machinery, interchangeable equipment, safety components, lifting accessories, chains, ropes and webbing, removable mechanical transmission devices and partly completed machinery (Machinery Directive, Art 1(1)).

Machinery is defined as “an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts of components, at least one of which moves, and which are joined together for a specific application.” (Machinery Directive, Art 2(a))

Certain products, such as most means of transport, machinery specially designed and constructed for military or police purposes and information technology equipment, are excluded from the scope of the Machinery Directive (Machinery Directive, Art 2(2)). The term “police purposes” is not defined. According to the official guidelines, this term would include machinery specially designed and construed for the purpose of maintaining order. It excludes ordinary machineries used by the police not specifically designed for that purpose. It is unclear whether it would extend to security products used to maintain order, but used by security guards, instead of police forces. The exemption focuses on the purpose of the machinery, rather than the person using it, so it could be argued that the exemption extends to machinery used by private parties.

Certain security products may thus fall under the scope of the Machinery Directive, if they have or is intended to have a drive system.

The Machinery Directive imposes obligations on manufacturers of machinery and their authorized representative if any. Manufacturer is defined as “any natural or legal person who designs and/or manufactures machinery or partly completed machinery covered by this Directive and is responsible for the conformity of the machinery or the partly completed machinery with this Directive with a view to its being placed on the market, under his own name or trademark or for his own use. In the absence of a manufacturer as defined above, any natural or legal person who places on the market or puts into service machinery or partly completed machinery covered by this Directive shall be considered a manufacturer” (Machinery Directive, Art 2(i)). Authorised representative is defined as “any natural or legal person established in the Community who has received a written mandate from the manufacturer to perform on his behalf all or part of the obligations and formalities connected with this Directive” (Machinery Directive, Art 2(j)).

---

3.2.7.5. Relation with liability

The Machinery Directive is not a liability programme but potentially affects liability exposure in opposite ways. On one hand, it can expand liability exposure where:

(i) it raises the applicable standards by requiring machinery to meet certain safety and performance requirements;
(ii) non-compliance with the regulatory standards constitutes breach of obligation or negligence per se, which may trigger liability exposure. If a product does not meet the Machinery Directive’s requirements, its manufacturer and/or distributor is exposed to fines. This, in turn, may constitute an argument to support a claim that the producer is liable under civil law for damage caused by the unsafe product.

On the other hand, compliance with the Machinery Directive could potentially limit effective liability exposure if:

(i) companies adopt measures to avoid that non-compliant machinery is placed on the market and to mitigate any risk related to non-compliant machinery already placed on the market;
(ii) a product that meets the requirements of the Machinery Directive may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with the regulatory standards does not preclude potential civil liability exposure; for example, the PLD does not provide for this, so it will not be a decisive factor.

3.2.7.6. Financial security and compensation mechanisms

The Machinery Directive does not provide for any mechanisms of financial security or compensation for producers. Section 6 of Annex XI requires the subscription of a civil liability insurance for the bodies designated by the Member States, unless that liability is assumed by the Member State in accordance with national law, or the Member State itself is directly responsible for the tests.

3.2.7.7. Applicability in time

The Directive entered into force in 2006. Member States had to transpose its provisions by 29 June 2008 and they became effective on 29 December 2009.

Member States may allow the placing on the market and the putting into service of portable cartridge operated fixing and other impact machinery which are in conformity with the national provisions in force upon adoption of the Machinery Directive until 29 June 2011 (Machinery Directive, Art 27).

3.2.7.8. Other relevant features

The Machinery Directive provides for market surveillance and a safeguard mechanism (Machinery Directive, Arts 4, 11, 17, and 23). Member States must conduct market surveillance activities and require manufacturers to end any non-compliance. If the non-compliance persists, Member States can restrict or prohibit the placing on the market of the relevant construction product concerned or order a product recall.

When the Commission considers that a harmonized standard does not satisfy the Annex I health and safety requirements it covers, the Commission may take measures requiring
Member States to prohibit or restrict the placing on the market of the machinery (Machinery Directive, Art 9(1)).

3.2.7.9. Conclusions Machinery Directive and relevance to the security industry

The Machinery Directive is a relevant instrument for the purpose of this Study. It can apply to those security products that have a drive system. The Machinery Directive, however, is not intended to address risks of terrorism or public security.

The standards and certification pursuant to the Machinery Directive are features that may be relevant to the security industry. Compliance with standards and post-marketing obligations could possibly result in limitation of liability.

The ‘police exemption’ (i.e. exemption from the Machinery Directive for machinery specially designed and constructed for police purposes) is a feature that could be used by analogy.

3.2.8. Construction Products Regulation 305/2011

3.2.8.1. Brief summary of the regime

Regulation 305/2011 on construction products114 (“CPR”) harmonizes conditions for the placing or making available on the market of construction products. It imposes basic safety and performance requirements, including mechanical resistance and stability, assessment by a notified body, and CE marking and regulates how to communicate the performance of construction products.

3.2.8.2. Key objectives

The objective of the CPR is to “achieve the proper functioning of the internal market for construction products by means of harmonised technical specifications to express the performance of construction products.” (CPR, recital 58)

3.2.8.3. Key instruments

(i) Design requirements

Construction products must comply with harmonized standards and technical assessments that implement basic performance and safety requirements set forth by the CPR, including mechanical resistance and stability, safety in case of fire, hygiene, health and the environment, accessibility and sustainable use of natural resources. Harmonized standards are established by the EU standardization bodies on the basis of requests issued by the Commission. If a construction product is not covered or not fully covered by such standards, a manufacturer can request the Technical Assessment Body to adopt a European technical assessment for that product (CPR, Arts 19 and following).

Manufacturers must also adopt procedures to ensure that series production “maintains the declared performance.” (CPR, Art 11(3)).

(ii) Informational, reporting, and disclosure requirements vis-à-vis government and/or customers and consumers
Manufacturers must develop and keep for 10 years technical documentation, draw up a declaration of performance and affix the CE marking to their products (CPR, Article 11(1) and (2)). This technical documentation and all information and documentation necessary to demonstrate compliance with the CPR must be available upon request to the national authorities (CPR, Article 11(8)).

They must also ensure the traceability of their products by marking them with an identification number, such as a serial number, and their contact information, or providing this information on an accompanying document (CPR, Article 11(4) and (5)).

They must also affix a CE-marking on a construction product draw up a declaration of performance (CPR, Arts 4–9), if the construction product is covered by a harmonized standard or if it conforms to a European Technical Assessment which has been issued for it, when such a product is placed on the market. The declaration of performance varies according to the particular harmonized technical specification covering the product.115

Finally, they must provide instructions and safety information with their products (CPR, Article 11(6)).

(iii) Post-marketing monitoring requirements and related reporting obligations
If appropriate, manufacturers must monitor products on the market by conducting sampling, keep a register of complaints, non-conforming products and product recalls, and inform distributors of such monitoring (CPR, Article 11(3)).

Manufacturers must also take all the necessary corrective measures, including product recall, if they consider or have reason to believe that products placed on the market are noncompliant.

3.2.8.4. Regulated activities or products

Construction products are defined as “any product or kit which is produced and placed on the market for incorporation in a permanent manner in construction works or parts thereof and the performance of which has an effect on the performance of the construction works with respect to the basic requirements for construction works” (CPR, Article 2.1).

Some security products may be incorporated in a permanent manner in buildings, such as alarm systems, and may have an effect on the performance of the construction, for example to address safety in case of fire. The CPR applies therefore to these security products.

As discussed above, manufacturers must draw up a declaration of performance and attach CE markings to construction products they place on the market. Furthermore, they need to put in place procedures that will ensure that series production maintains the declared performance (article 11.3). If manufactures have reason to believe that a construction product they placed on the market does not conform with any of the provision of the CPR, they must immediately try to remedy or, if necessary, withdraw the product from the market. If the product presents a risk, national competent authorities must be notified (article 11.7).

---

115 CPR, Articles 8-9. See also the Construction Products Association (CPA), the British Board of Agreement (BBA), the British Standards Institution (BSI) and FBE Management Limited in consultation with the Trading Standards Institute (TSI), ‘Guidance Note on the Construction Products Regulation’ (April 2012) 3.
The CPR imposes obligations on all economic operators, covering manufacturers, their representative (authorised representative), if any, importers and distributors. Manufacturer is defined as “any natural or legal person who manufactures a construction product or who has such a product designed or manufactured, and markets that product under his name or trademark.” (CPR, Art 2(19))

Importers and distributors have similar obligations than manufacturers, as described above (CPR, Arts 13-14). Importer is defined as “any natural or legal person established within the Union, who places a construction product from a third country on the Union market” (CPR, Art 2(21)) and distributor as “any natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a construction product available on the market” (CPR, Art 2(20)).

3.2.8.5. **Relation with liability**

The CPR is not a liability programme but potentially affects liability exposure in opposite ways. On one hand, it can expand liability exposure where:

(i) it raises the applicable standards by requiring construction products to meet certain safety and performance requirements;

(ii) non-compliance with the regulatory standards constitutes breach of obligation or negligence per se, which may trigger liability exposure. If a product does not meet the CPR’s requirements, its manufacturer and/or distributor is exposed to fines. This, in turn, may constitute an argument to support a claim that the producer is liable under civil for damage caused by the unsafe product.

On the other hand, compliance with the CPR could potentially limit effective liability exposure if:

(i) companies adopt measures to avoid that non-compliant construction products are being placed on the market and to mitigate any risk related to non-compliant construction products already placed on the market;

(ii) a product that meets the requirements of the CPR may de facto be regarded as not being “defective” under the PLD. Note, however, that compliance with the regulatory standards does not preclude potential civil liability exposure; for example, the PLD does not provide for this, so it will not be a decisive factor.

3.2.8.6. **Financial security and compensation mechanisms**

The CPR does not provide for any mechanisms of financial security or compensation for producers. All notified bodies must take out liability insurance unless liability is assumed by the Member State in accordance with national law, or the Member State itself is directly responsible for the assessment and/or the verification performed (CPR, Art 43(9)).

3.2.8.7. **Applicability in time**

The CPR entered into force in 2011. However, most of its provisions only apply from 1 July 2013 onwards.
The CPR repealed Directive 89/106/EEC and contains a number of transitional provisions (CPR, Art 66):

- Construction products which have been placed on the market in before 1 July 2013 in accordance with Directive 89/106/EEC shall be deemed to comply with the CPR;
- Manufacturers may draw up a declaration of performance on the basis of a certificate of conformity or a declaration of conformity, which has been issued before 1 July 2013 in accordance with Directive 89/106/EEC;
- Guidelines for European technical approval published before 1 July 2013 in accordance with Directive 89/106/EEC may be used as European Assessment Documents;
- Manufacturers and importers may use European technical approvals issued in accordance with Directive 89/106/EEC before 1 July 2013 as European technical assessments throughout the period of validity of those approvals.

3.2.8.8. Other relevant features

The CPR provides for market surveillance and a safeguard mechanism (CPR, Arts 56-59). Member States must conduct market surveillance activities and require manufacturers to end any non-compliance. If the non-compliance persists, Member States can restrict or prohibit the placing on the market of the relevant construction product concerned or order a product recall.

3.2.8.9. Conclusions Construction Products Regulation and relevance to the security industry

The CPR is a relevant instrument for the purpose of this study. It applies to some security products that are incorporated in buildings, and has an effect on their performance, such as safety in case of fire. The CPR is, however, not intended to address risks of terrorism or public security.

The standards and certification pursuant to the CPR are features that may be relevant to the security industry. Compliance with standards and post-marketing obligations could possibly result in limitation of liability by reducing physical risk.

3.3. Regulation 785/2004 on Insurance Requirements for Air Carriers and Aircraft Operators

3.3.1. Summary of the Regime

Regulation 785/2004 establishes a framework on the minimum insurance requirements from air carriers and aircraft operators to cover their liability in respect of passengers, baggage, cargo and third parties.

---

117 This corresponds to Task 1.3 of Work Package 1 of the Invitation to Tender.
3.3.2. Key Objectives

This focus on insurance requirements in the aviation industry follows the terrorist attack of 11 September 2001 in the US. This regulation aims both at consumer protection and at ensuring a level playing field for air carriers.118 This is under the background of the harmonized regulatory framework for aviation in the EU since 1988. The implementation of the third liberalization package covering licensing, market access and fares and rates has realized the full liberalization of the EU aviation market.119 The Commission of the European Communities’ competence to manage the external aviation relations are the EU was confirmed by the ECJ in 2002.120 Now the EU’s aviation regulatory framework has extended to different areas, including passenger, environmental protection, insurance safety and security.121

3.3.3. Key Instruments

To fulfil the obligation to provide insurance coverage, the air carriers or aircraft operators are required to provide a deposit of and insurance certificate or other evidence of valid insurance to the competent authorities of the MS. For the Community air carriers/aircraft operators, the MS concerned is the MS which has granted the operating license or where the aircraft is registered. For the non-Community aircraft, MS means the MS to or from which the flights are operated.

The Regulation requires MS to ensure that the obligation to maintain insurance is fulfilled. It also allows MS to request additional evidence from the air carrier/aircraft operator.122 The regulation also has provisions related to sanctions. It requires sanctions to be effective, proportional and dissuasive. The sanctions may concern the withdrawal of the operating license for Community air carriers and the refusal of the right to land on the territory of a MS for the non-Community ones. A MS can also refuse the take-off of an aircraft if it is not satisfied that the conditions of the Regulation are met.

3.3.4. Regulated Entities and Activities or Products

The application of this regulation is very broad, covering “all air carriers and […] all aircraft operators flying within, into, out of, or over territory of a Member State”.123 It defines an “air carrier” as “an air transport undertaking with a valid operating license”124 and an “aircraft operator” as “the person or entity, not being an air carrier, who has continual effective disposal of the use or operation of the aircraft”.125 The air carriers or aircraft operators are not necessarily European. This regulation does not apply with respect to flights over the territory of the Member States carried out by non-Community air carriers and by aircraft operators using aircraft registered outside the Community, which do not involve a landing on, or take-off from such territory.126

---

118 Preamble (1) (3).
120 Id., 27-38.
121 Smithies 2007.
122 Article 8(3).
123 Article 2(1).
124 Article 3(a).
125 Article 3(c).
126 Article 6(4).
3.3.5. Relation with Liability

This regulation concerns the coverage of liability in respect of passengers, baggage, cargo and third parties. However, this regulation itself does not provide liability rules. Hence, how aviation liability is decided still depends on the international treaties, other EU laws and domestic laws in MS. Two types of liability are involved: liability for passengers, baggage and cargo and liability for third parties.

There are two sets of international conventions prescribing liability in the aviation industry: the 1952 Rome Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (hereinafter Rome Convention) and the Convention for the Unification of Certain Rules for International Carriage by Air (Montreal Convention). The Rome Convention establishes liability for damage suffered on the surface due to an aircraft flight or any person or thing falling there from. The Montreal Convention applies to the international carriage of persons, baggage or cargo. Many European countries are Member States of the Rome Convention. The European Community approved the Montreal Convention and the Member States of the EU need to ratify this convention.

Some European legislation is also promulgated on aviation liability. For example, Council Regulation No. 2027/97 on Air Carrier Liability in respect of the Carriage of Passengers and their Baggage by Air harmonized the liability of Community air carriers to passengers. In response to the conclusion of the Montreal Convention in 1999, Regulation No.889/2002 was promulgated to bring the Community law in line with the international convention.

The regulation 785/2004 does not contain a liability framework itself, but only establishes an obligation to seek liability insurance coverage. It states clearly that the regulation is without prejudice to liability rules from international conventions, community law and national law of MS. Hence to figure out the basis liability of the aviation industry in the EU, one needs to look at other legal sources. The liability under the Rome Convention and the Montreal Convention will be further analyzed in Chapter 5.

Since this regulation has no direct provision with regard to liability, for the liability issues and its relevance with regulation, one needs to look at the applicable international and domestic laws.

3.3.6. Financial Security and Compensation Mechanisms

Regulation 785/2004 requires air carriers/ aircraft operators flying within, into, out of or over the territory of a MS to maintain insurance as regards their aviation liability for passengers, baggage, cargo and third parties. The regulation excludes application to State aircraft, captive balloons, kites and some small aircrafts.

---

127 These treaties concerning civil aviation will be discussed below in Chapter 5, section 5.1.
129 Article 4(3).
130 Especially the Rome Convention and the Montreal Convention. The above analysis has shown that the EU regulations make EU law in line with the Montreal Convention. Hence the Montreal Convention is the main source shaping the liability for damage to passengers, baggage and cargo. Many EU countries are also member of the Rome Convention.
131 Article 4.
132 Article 2(2).
The Regulation contains some compliance provisions. The air carriers/aircraft operators shall provide a deposit of an insurance certificate or other evidence of valid insurance to the competent authorities of the MS concerned. The regulation prescribes that in case of insurance-market failure, the Commission may determine the appropriate measures to realize the obligation of providing insurance coverage.

A minimum insurance requirement is established under the Regulation according to the types of liability.

<table>
<thead>
<tr>
<th>Minimum requirement</th>
<th>Liability for passengers</th>
<th>Liability for baggage</th>
<th>Liability for cargo</th>
<th>Liability for third parties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>250,000 SDRs per passenger; for aircraft smaller than MTOM of 2700 kg, MS may set a lower amount, but no less than 100, 000 SDRs per passenger</td>
<td>1000 SDRs per passenger</td>
<td>17 SDRs per kilogram</td>
<td>From 0.75 Million SDRs to 700 SDRs, depending on the size of aircrafts</td>
</tr>
</tbody>
</table>

The minimum requirement under the first three types does not apply to flights over the territory of the MS carried out by non-Community air carriers/aircraft operators which do not involve a landing on, or take-off from such territory. The preamble of this regulation takes note of this situation. Though it is not binding, it shows the role of international law in these cases: the overflown MS may in accordance with international law, request evidence of compliance with the insurance requirement.

According to the Regulation, the air carriers/aircraft operators shall insure the risks of acts of war, terrorism, hijacking, acts of sabotage, unlawful seizure of the aircraft and civil commotion. However, in these cases, the insurance coverage may not be available on a per-accident basis. Under this situation, the regulation allows the use of insurance policies on an aggregate basis.

### 3.3.7. Transition

Article 11 of the Regulation stipulates that it shall enter into force twelve months following the dates of its publication in the Official Journal. Since the publication took place on 30 April 2004 the entry into force was on 30 April 2005. The Regulation hence carries no retrospective effects.

### 3.3.8. Conclusions Regulation 785/2004 and Relevance to the Security Industry

This regulation has relevance to security industry, especially the products/services used on the aircraft to identify, prevent and respond to safety threats. The regulation requires air carriers/aircraft operators to seek insurance coverage for their potential liability. The insured
risks include acts of war, terrorism, hijacking, acts of sabotage, unlawful seizure of aircraft and civil commotion. This may concern the security industry when damage is caused by the failure of security products/services to provide protection from terrorism and organized crimes.

However, one should keep in mind that the insurance obligations apply to air carriers and aircraft operators. Victims may hence be compensated under the insurance coverage of air carriers and aircraft operators and in that sense have no incentive to bring a liability suit against the security industry (assuming that the collateral source rule applies and the compensation level under civil liability law does not exceed the compensation provided through the insurance). Thus, the mandatory insurance requirement under this regulation may indeed reduce the liability exposure of the security industry. The mandatory insurance leads to an effective channelling of liability to the air carriers and aircraft operators. Note, however, that the mandatory insurance coverage, in principle, does not include the security industry.


The Commission Recommendation of 5 June 2008 concerning the limitation of the civil liability of statutory auditors and audit firms (2008/437/EC) can be considered as a reaction to (actual and potential) auditors’ liability problems in the wake of the many corporate and accounting scandals of the early 2000s. Indeed, recent studies by the US General Accountability Office, London Economics, and the OECD have all concluded that the big accounting firms outside of the Big Four (PwC, Deloitte, KPMG, Ernst & Young) are unwilling to enter the market for audits of quoted and large companies partly because they fear potential liability claims.

This is problematic, as competition in the audit sector is currently limited, with only four accounting networks active in the market for audits of quoted and large companies. Moreover, one has to take into account that an accounting firm cannot be both auditor and consultant for one and the same client. For big audit clients, this limits the number of auditors to choose from to a maximum of three. In reality there may be fewer options, because not all of the Big Four firms are equally specialized in certain sectors, such as the financial sector.

The explanation for the fact that there is currently a Big Four, whereas there used to be a Big Eight until the late 1980s, can be found in a series of mergers that took place between the big accounting networks and the demise of Arthur Andersen in 2002 as a result of the Enron scandal. It is unlikely that yet another merger between these remaining four accounting firms would be allowed today; however, it is not unthinkable that one of them collapses due to liability claims.

One of the main purposes of the US Government Accountability Office study conducted in 2003, as in the later studies by London Economics and the OECD, was to find out whether the

---

138 It is not a legal channelling in the sense that the liability suit against the security industry is still possible, but rather an economic channelling provided via the mandatory insurance.

139 This corresponds to Task 1.4 of Work Package 1 of the Invitation to Tender.

140 Examples of accounting scandals include Worldcom, Enron, Ahold, Parmalat, and Satyam Computers. Many different accounting firms were involved in these scandals, including all of the Big Four networks.

141 GAO 2003, London Economics 2006, Philipsen 2009. These so-called ‘middle-tier firms’ include internationally operating networks such as Grant Thornton and BDO. Other barriers to entry (besides the exposure to unlimited liability) mentioned by these middle-tier firms are reputation and capacity.

142 London Economics 2006, p. 31-32.

growth of alternative audit firms (e.g. middle-tier firms) could be encouraged, by reducing some of the risks linked to the audits for large and quoted companies. In that context *inter alia* capping auditors’ liability was considered. Academics and others interviewed in the context of the GAO study argued that a liability cap would potentially reduce the incentives for auditors to conduct quality work, while it could also limit investors’ ability to recoup losses they incurred if an auditor was found to have committed fraud. On the first point, one could argue that quality regulation, such as the Sarbanes-Oxley Act in the United States and the 2006 Audit Directive in the EU, is a more suitable instrument to guarantee a minimum quality of audit services. However, Law and Economics literature has shown that liability rules may provide an important deterrent function in that respect, by making auditors take optimal care in performing their ‘gatekeeping’ function.

Some academics have argued that because of special characteristics of auditors’ liability, the potentially negative effects of liability caps are mitigated. Instead, such caps might even induce efficient levels of care taken by auditors. Unlimited liability, on the other hand, would induce auditors to exert excessive care. The special characteristics of auditors’ liability, which are central to reaching this conclusion, include: (1) the importance of reputation effects; (2) liability only in cases of negligence; (3) vaguely defined standards of due care; and (4) overcompensation as a result of liability for pure economic loss and wrong assessment of damages.

In Europe, the Commission – following the independent study by London Economics and a public consultation – issued Recommendation 2008/437/EC concerning the limitation of the civil liability of auditors.

### 3.4.1. Brief summary of the regime

The preamble to Recommendation 2008/437/EC provides the context of the regime, which (as was stated above) is linked to problems of competition:

“Since unlimited joint and several liability may deter audit firms and networks from entering the international audit market for listed companies in the Community, there is little prospect of new audit networks emerging which are in a position to conduct statutory audits of such companies.”

Article 2 of the Recommendation states that the civil liability of statutory auditors and audit firms arising from a breach of their professional duties should be limited. The only exception is intentional breach of duties by the auditor.

Article 5 of Recommendation 2008/437/EC provides the methods for limiting liability, leaving it to the Member States to choose one or more of these options, depending on which methods are most suitable for their respective civil liability systems:

- establishment of a maximum financial amount or of a formula allowing for the calculation of such an amount;

---

144 Philipsen 2009, p. 28.
145 Directive 2006/43/EC. See on the relation between regulation and liability section 7 below.
146 See generally Philipsen 2012.
147 Bigus 2008 and references therein.
148 No. (3) of the Preamble to Recommendation 2008/437/EC.
- establishment of a set of principles by virtue of which a statutory auditor or an audit firm is not liable beyond its actual contribution to the loss suffered by a claimant and is accordingly not jointly and severally liable with other wrongdoers;
- provision allowing any company to be audited and the statutory auditor to determine a limitation of liability in an agreement.

In other words, Member States are allowed to choose between a liability cap, a system of proportionate liability, and a form of contractual limitation. If the latter option is chosen, it is **inter alia** required that the agreement is subject to judicial review and that the limitation of liability is published in the notes to the accounts of the audited company. Member States also have to take into account the impact on financial markets and investors of the option that is chosen, as well as its impact on access to the audit market, quality of audits, insurability of risks and the companies to be audited. 

### 3.4.2. Basis of liability

There are many variations between civil liability systems of Member States. Recommendation 2008/437/EC only lists options to limit liability, leaving the choice to the Member States.

Auditors or audit firms are usually held liable only in cases of negligence. Bigus (2008) in that respect has pointed out that standards of due care in auditing are sometimes “vaguely defined”, resulting in the problem that “the auditor does not always exactly know ex ante whether he will be held negligent ex post or not”. PricewaterhouseCoopers has noted that potentially disastrous liability claims are a cause for concern, when auditors face judicial actions that would penalize firms “beyond the level of their responsibility”. PwC therefore, not surprisingly, supported the system of contractual proportionate liability that was introduced in the UK some years ago, as well as Commission Recommendation 2008/437/EC, central to our study.

### 3.4.3. Liable persons (attribution of liability)

London Economics (2006) noted on attribution of liability that “[o]nce a firm has exhausted the limited cover provided by the network’s captive and commercial insurers, the remaining source of funds is essentially the partners’ income. At issue then for a firm is how large an income cut partners would be willing to take before leaving the firm in drove, resulting in the collapse of the firm.” Moreover, reputational effects are very important in the audit market. “In cases where the survival of a firm, considered to be a linchpin of a network, is at risk because of a large claim against it, partners of other firms in the network may need to assist financially the threatened firm to ensure the survival of the network.”

As mentioned in the preamble to Recommendation 2008/437/EC, “unlimited joint and several liability” may be imposed not only on individual audit firms or accountants belonging to that firm, but also on the accounting network. Whether also vicarious liability can be imposed on

---

149 Article 6 of Recommendation 2008/437/EC.
150 Article 7 of Recommendation 2008/437/EC.
152 PricewaterhouseCoopers 2008, p. 3.
153 See on insurance below, section 8.
an international accounting network for damage caused by a firm belonging to the national network, depends on the possibilities to ‘pierce the corporate veil’, as on the national level limited liability constructions for corporations are in place. Although the big accounting networks develop their audit and accounting standards at the international level, precisely in order to signal a shared quality (branding), it remains a question whether this is sufficient to disregard the limited liability at national level.\textsuperscript{156}

3.4.4. Damage covered

The Recommendation does not state anything on the amount of damages that should be covered. Article 2(4) of Recommendation 2008/437/EC, however, provides that “any limitation of civil liability should not prevent injured parties from being fairly compensated”, despite the fact that liability is now limited.

We mentioned above that according to Bigus (2008) there is often overcompensation as a result of liability for pure economic loss and due to wrong assessment of damages.

London Economics (2006) found that before Recommendation 2008/437/EC was implemented, a small number of EU Member States already had a statutory limitation on auditors’ liability: Austria, Belgium, Germany, Greece and Slovenia.\textsuperscript{157}

3.4.5. Exclusions and defenses

The Recommendation does not deal with exclusions and defences.

3.4.6. Causation

Causation is dealt with at Member State level.

3.4.7. Relation with regulation

The 2006 Audit Directive\textsuperscript{158} - which deals \textit{inter alia} with educational requirements, professional ethics and public oversight - establishes a minimum harmonisation of statutory audit requirements. To the extent that these requirements lead to higher quality standards for audit services in a particular Member State, this increases the likelihood that auditors or audit firms not meeting these standards will be confronted with tort claims. In other words: liability will be expanded. Hence there is a direct link between the Audit Directive and the potential liability risks faced by auditors.

Article 31 of the Audit Directive stated that the Commission needs to report on the impact of the national liability rules for the carrying out of statutory audits on European capital markets and on the insurance conditions for statutory auditors and audit firms.

\textsuperscript{156} This discussion is going beyond the scope of this study. For an analysis of the theoretical possibilities to apply vicarious liability to audit firms, see Steins Bisschop & Olaerts 2010. In addition to discussing vicarious liability, the authors also discuss whether there could be a ‘principal-agent’ relationship in accounting networks, resulting in the principal (i.e. the international accounting network) being held liable for actions taken by its agents.

\textsuperscript{157} London Economics 2006, p. xxiii.

\textsuperscript{158} Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts.
3.4.8. Financial security and compensation mechanisms

From the perspective of audit firms that are faced with liability claims, there is a clear link with the availability, costs and conditions of liability insurance. The London Economics study conducted for DG Internal Market in 2006 concluded that “[t]he level of auditor liability insurance available for higher limits from the commercial market has fallen sharply in recent years in terms of both the level and amount of insurance, and the conditions under which the insurance cover is effective.” Moreover, the price of that insurance had risen substantially, doubling over a period of five years in the case of reinsurance provided to the captives of the Big Four networks.\(^\text{159}\)

Also in the US context, the Government Accountability Office in 2003 concluded that the accounting scandals and escalating litigation involving accounting firms had resulted in an increase in insurance costs, because insurance companies saw increased risk and uncertainty from insuring firms that audited public companies.\(^\text{160}\)

From the perspective of audit clients (i.e. the audited companies) and their shareholders, the effects of a breach of professional duties by the auditor may or may not be financially dramatic, depending on the availability of alternative auditors and any reputational effects spilling over to the audited company.

Articles 6 and 7 of Recommendation 2008/437/EC are aimed at the protection of the interests of the audited firm and its investors, as well as those of third parties. Article 7 provides that “[b]efore adopting measures implementing any of the [three methods to limit liability], a Member State should take into account the impact on financial markets and investors and on conditions for access to the market of statutory audit for listed companies, as well as the impact on audit quality, insurability of risks and the companies to be audited” (emphasis added). Article 6 provides that, if contractual limitation of liability is chosen: (1) the agreement is subject to judicial review; (2) the essence of the agreement is published in the notes to the annual accounts of the audited company, (3) the limitation is decided collectively by the members of the relevant administrative, management and supervisory bodies of the audited company; and (4) the decision is approved by the shareholders of the company to be audited.

3.4.9. Rules of evidence

Rules of evidence are decided on a Member State level.

3.4.10. Jurisdictional and procedural issues

Recommendation 2008/437/EC does not deal with jurisdictional and procedural issues. Since this is a recommendation there are no specific rules with respect to entry into force. Article 8 merely invites Member States to inform the Commission of actions taken in light of this recommendation by 5 June 2010, two years after the promulgation of the Directive.

\(^\text{159}\) London Economics 2006, p. xxi.  
\(^\text{160}\) GAO 2003, p. 49.
3.4.11. Conclusions Auditor’s Liability and implications for security industry

Auditing firms are not part of the security industry and hence at first blush this recommendation does not seem relevant for the security industry. However, the analysis of this Recommendation and, perhaps even more, a study of the literature on auditors’ liability is highly relevant for the security industry. Indeed, there are some important parallels. Like the security industry, auditors claimed that they were unreasonably exposed to increasing liability. The traditional argument that a financial limit on liability will reduce incentives of operators may not apply to auditors because reputational effects may play a role, liability is limited to negligence, vague standards apply and there is a serious risk of overcompensation as a result of liability for pure economic loss and the wrong assessment of damages. The question then arises to what extent these criteria also apply to the security industry. This is a point that will be taken up further in Chapter 8 when formulating legal and technical options for implementing a feasible third party liability regime in the EU. The question will be asked whether the criteria that justified a financial limit on liability for the auditors also apply to the security industry. There we will further analyse to what extent factors such as reputation may also provide additional incentives, whether standards for liability are indeed vague and whether there is a serious risk of overcompensation.

Further, the three methods suggested in the recommendation for limiting liability may be relevant to the security industry.

Moreover, the regulatory approach followed by the EU in the auditing sector is interesting from various perspectives. First of all, no formal EU action (like a regulation or directive) aiming at harmonisation is taken, but Member States are merely recommended to follow the strategy suggested in Recommendation 2008/437/EC. Second, the Recommendation clearly provides different options to follow for Member States if they would choose to limit auditors’ liability. Hence, the recommendation provides a lot of flexibility to Member States, respecting the principle of subsidiarity. Again, this is an important trade-off to be addressed in Chapter 8: on the one hand, there are many arguments in favour of this flexible approach followed in the recommendation (a flexible, optional approach, respecting the subsidiarity principle). On the other hand operators (auditors in the case of the Recommendation or the security industry in our study) may with a flexible, optional recommendation not be sure that Member States will follow it and thus that their liability exposure is truly limited. A recommendation clearly does not aim at reaching a level-playing field.

Finally, the argument (as suggested by Bigus) that especially a wrong assessment of damages or large exposure to economic loss can expand the exposure to liability is an interesting one. This also shows that if one would seek methods to limit the liability exposure of the security industry, one method is to look for a financial limit on liability; another one is to limit particular heads of damage.

Finally, the case of the auditors is interesting given the relationship with regulation. It confirms a general point addressed in law and economics literature, i.e. that a combination of regulation and liability rules may be required in order to move to an efficient level of care taken by auditors while performing statutory audits. On the other hand it leads to a general point often mentioned when discussing the regulatory regimes (more particularly above in section 3.2) that the combination of liability and regulation could either expand liability (in the case that regulatory standards are violated) or potentially limit liability (in the case the regulatory standards are complied with and this is considered as proof of following the due care standard in a liability case).
3.5. Legal Analysis of Further Secondary European Law

This section focuses on additional EU legislation that limits or expands, as a matter of law or as a matter of fact, third party liability exposure. It is not expected that any EU legislation directly limits or expands third party liability, so the focus is on EU law that indirectly or as a matter of fact may limit or expand liability exposure. As a practical matter, this task analyzes the EU law that is concerned with jurisdiction of the courts, enforcement of judgments, civil procedure and compensation, and the law governing contracts.

The EU legislation relevant to these topics has been enacted pursuant to the EU policy regarding judicial cooperation in civil matters, which is aimed at promoting closer cooperation between the national authorities. The legislation enacted pursuant to this policy seeks to eliminate obstacles deriving from incompatibilities between the various legal and administrative systems, and thus facilitate access to justice. A cornerstone is the principle of mutual recognition and enforcement of judgments and of decisions resulting from extrajudicial cases. Thus, rather than limiting third party liability exposure, this legislation is intended to facilitate cross-border litigation and thus, indirectly, to expand liability exposure as a matter of fact.

We use the common format for the analysis of liability regimes set forth in [Appendix 1], but only the section on jurisdictional and procedural issues. Thus, the following key questions are addressed:

- Which courts have jurisdiction to hear claims under the regime (courts of the plaintiff’s home country, and courts of the defendant’s home country);
- How can a judgment obtained in one Member State be recognized and enforced in another in another Member State;
- Are there any specific rules regarding cross-border litigation (where the plaintiff and defendant are based in different Member States) or compensation;
- Can multiple claims be managed to increase efficiency (e.g. centralize claims in one court, or suspend proceedings until one claim has been resolved, etc.);
- How is the applicable law determined.

These European laws seek to eliminate obstacles deriving from incompatibilities between the various legal and administrative systems, and thus facilitate access to justice. Its cornerstone is the principle of mutual recognition and enforcement of judgements and of decisions resulting from extrajudicial cases. Judicial cooperation in civil matters contributes to the area of justice, freedom and security, as governed by the Treaty on the Functioning of the European Union (Title V). The following EU laws are analyzed in this section:

Jurisdiction of courts and recognition and enforcement of judgments:

---

161 This corresponds to Task 1.5 of Work Package 1 of the Invitation to Tender.
Civil procedure and compensation:
- Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters;

Applicable law:
- Regulation (EC) No 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I);

We first provide a brief summary of the key provisions and then focus on the issues identified above. As in other parts of this study, particular attention is paid to features that could factor into feasible policy options to be considered by the European Commission with respect to SI providers’ TPL.

Directive 2004/80 on compensation to crime victims does not relate to civil procedure, but is discussed because it may affect third party liability exposure, for instance, if compensation obtained through other mechanism reduces the amounts that can be recovered in civil litigation (also called the “collateral source” rule).

3.5.1. Regulation 44/2001 on the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I)

3.5.1.1. Brief summary of the regime

Regulation 44/2001\(^{162}\) (“Brussels I Regulation”) establishes rules to determine the jurisdiction competent in civil and commercial matters and for the recognition and enforcement of judgments.

Parties may agree on the competent jurisdiction, unless the Brussels I Regulation grants exclusive jurisdiction to the courts of a Member States (e.g., cases related to rights in rem in immovable property) or limit such rights (e.g., consumer or insurance contracts) (Brussels I Regulation, Art 23).

In the absence of contract, the default rule is the jurisdiction of the Member State where the defendant is domiciled (Brussels I Regulation, Art 2), unless the Brussels I Regulation gives special jurisdictions to the courts of another Member States.

In contractual matters, the seller of a security product may also be sued in the Member State where the product was or should have been delivered and a provider of security services may also be sued in the Member State where the services were or should have been provided (Brussels I Regulation, Art 5(1)).

In extra-contractual matters, the plaintiff may also file a legal proceedings in the courts for the place where the harmful event occurred (Brussels I Regulation, Art 5(3)) or the court seized of a criminal proceedings for related civil claims, if such court has jurisdiction for civil proceedings (Brussels I Regulation, Art 5(4)). This rule could, for example, applies in the case of terrorism.

Insurers may be sued in the Member State of their domicile, in the Member State where the plaintiff is domiciled, if it is a policy holder, the insured or a beneficiary or, for liability insurance, in the Member State where the harmful even occurred (Brussels I Regulation, Arts 8-14).

In the case of lis pendens, all courts must suspend proceedings, except the court first seized, and decline jurisdiction if the court first seized declares itself competent (Brussels I Regulation, Art 27). A similar rule is optional if the various legal proceedings cover related, but not identical actions.

If there are multiple defendants, including a security company, it can be sued in any Member State where a defendant is domiciled, if the claims are closely connected (Brussels I Regulation, Art 6(1)). In the case of third party proceedings, such as an action on a warranty or guarantee, a security company may also be sued in the court seized of the original proceedings (Brussels I Regulation, Art 6(2)).

A judgment from a court in a Member State must be recognized in other Member States with limited exceptions, such as judgments manifestly contrary to public policy (Brussels I Regulation, Arts 33-37). It may also be enforced in other Member States, provided that it has been declared enforceable by a court of that Member State after assessment that the application for enforceability meets certain formal requirements (Brussels I Regulation, Arts 38-).

3.5.1.2. Applicability in time

The Brussels I Regulation entered into force on 1 March 2002 and applies to legal proceedings instituted after that date or, in certain cases, to judgements given after dates in proceedings started before (Brussels I Regulation, Art 66).

163 For further discussion of this criteria, see Magnus and Mankowski 2007, p. 202 ff..
3.5.1.3. Conclusions Regulation 44/2001 and relevance to the security industry

The Brussels I Regulation harmonizes rules that determine the jurisdiction competent for civil and commercial matters. It is thus applicable to claims from victims of terrorism and customers against the security industry. The Brussels I Regulation allows parties to select a governing law that is either in favour of or disadvantageous to the security company involved. It also facilitates cross-border litigation which, indirectly, expands liability exposure. A clear regime for establishing the selection of jurisdiction and how to recognize and enforce judgment saves time and transaction costs. The Brussels I Regulation also decreases the risk for the security industry to be sued in various countries for the same event of terrorism, since rules on tort and contractual claims as well as on lis pendens favour a single forum for the same event.

The place where the damage occurred can, however, sometimes be totally unpredictable in the case of a terrorist act involving means of transportation (e.g., airplane), which may make it difficult for the security industry to determine in advance which law will apply.

3.5.2. Regulation 2201/2003 on the jurisdiction and the recognition and enforcement of judgments in matrimonial matters and matters of parental responsibility (Brussels II)

3.5.2.1. Brief summary of the regime

Regulation 2201/2003164 ("Brussels II Regulation") establishes rules to determine the jurisdiction competent in matrimonial matters, including divorce, and matters of parental responsibility and for the recognition and enforcement of judgments in these matters.

Courts of the Member State of habitual residence of the child are competent for matters related to parental responsibility, with limited exceptions (Brussels II Regulation, Arts 8-15).

In cases between spouses, including divorce, jurisdiction lies with the court of the Member State:

“(a) in whose territory:
- the spouses are habitually resident, or
- the spouses were last habitually resident, insofar as one of them still resides there, or
- the respondent is habitually resident, or
- in the event of a joint application, either of the spouses is habitually resident, or
- the applicant is habitually resident if he or she resided there for at least a year immediately before the application was made, or
- the applicant is habitually resident if he or she resided there for at least six months immediately before the application was made and is either a national of the Member State in question or, in the case of the United Kingdom and Ireland, has his or her ‘domicile’ there;
(b) of the nationality of both spouses or, in the case of the United Kingdom and Ireland, of the ‘domicile’ of both spouses.” (Brussels II Regulation, Art 3(1)).

A judgment from a court in a Member State must be recognized in other Member States without any special procedure, with limited exceptions, such as judgments manifestly contrary to public policy (Brussels II Regulation, Arts 21-27). It may also be enforced in other

Member States, provided that it has been declared enforceable by a court of that Member State after a limited assessment that can reject such declaration for similar reasons as for recognition (Brussels II Regulation, Arts 28-36). Certain judgments must, however, be automatically enforced without the need for a declaration of enforceability (Brussels II Regulation, Arts 40-42), such as a judgement on the return of a child.

The Brussels II Regulation also requires Member States to cooperate in matters of parental responsibility (Brussels II Regulation, Arts 53-58).

3.5.2.2. Applicability in time

The Brussels II Regulation repeals Regulation 1347/2000. It entered into force on 1 August 2004 and applied to legal proceedings instituted from 1 March 2005, with limited exceptions for judgments given before that date (Brussels II Regulation, Art 64).

The Brussels II Regulation entered into force on 1 March 2002 and applies to legal proceedings instituted after that date or, in certain cases, to judgements given after dates in proceedings started before (Brussels I Regulation, Art 66).

3.5.2.3. Conclusions Regulation 2201/2003 and relevance to the security industry

The Brussels II Regulation harmonizes rules that determine the jurisdiction competent for matrimonial matters and matters of parental responsibility and the rules related to recognition and enforcement of judgments in these matters. It does not apply to claims related to terrorists acts and does not offer mechanism that may be of interest by analogy, except, possibly, against defendants to accelerate compensation of victims.

3.5.3. Regulation 1393/2007 on the service of judicial and extrajudicial documents

3.5.3.1. Brief summary of the regime

Regulation 1393/2007 on the service of judicial and extrajudicial documents165 (“Service Regulation”) provides a procedure for the service of judicial and extrajudicial documents, such as writ of summons, across Europe in civil and commercial matters. Member States agencies are responsible to assess a request to serve documents and transfer such documents. The receiving agency must serve the document or have it served within one month of receipt (Service Regulation, Art 7(2)). A Member State may also effect service of documents via consular or diplomatic channels or directly using registered post with a receipt or via officers (Service Regulation, Arts 12-14).

The addressee may refuse to receive the document if it is not translated into a language that he/she understands or the official language of the Member State or of the place where service is to be effected (Service Regulation, Art 8). Translation is at the cost of the applicant (Service Regulation, Art 5).

3.5.3.2. Applicability in time


3.5.3.3. Conclusions Regulation 1393/2007 and relevance to the security industry

The Service Regulation facilitates service of judicial and extrajudicial documents across Europe. It may have a positive impact in the case of cross-border litigation involving terrorist cases and the security industry by allowing and facilitating the handling of cross-border litigation.

3.5.4. Regulation 1206/2001 on cooperation in the taking of evidence

3.5.4.1. Brief summary of the regime

Regulation 1206/2001 on cooperation in the taking of evidence\(^\text{166}\) (“Evidence Regulation”) authorizes and facilitates requests from a national court to obtain evidence from a court located in another Member States or to take direct evidence in that Member State. The requested evidence must be intended for use in judicial proceedings (Evidence Regulation, Art 1(2)).

The request to a court to take evidence is made directly to the requested court in another Member State (Evidence Regulation, Art 2). The request must be executed within 90 days (Evidence Regulation, Art 10(1); Art 16 provides a procedure in the case of delay) or, if rejected, the rejection must be communicated within 60 days. The request may only be rejected in limited cases, including if the request is incomplete or if a person of whom a hearing has been requested claims a right to refuse, or a prohibition, from giving evidence (Evidence Regulation, Arts 8 and 14).

Member States must designate a central body responsible for facilitating this cooperation (Evidence Regulation, Art 3). This central body is competent to decide on request from a court to take direct evidence within 30 days from receipt (Evidence Regulation, Art 17(4)). The request may be rejected in limited cases, including in the case of an incomplete request or if the direct taking of evidence is contrary to fundamental principles of law in that Member State (Evidence Regulation, Art 17(5)).

3.5.4.2. Applicability in time

The Evidence Regulation entered into force on 1 July 2001 and the main rules applied from 1 January 2004.

3.5.4.3. Conclusions Regulation 1206/2001 and relevance to the security industry

The Evidence Regulation facilitates the exchange and the taking of evidence across Europe in civil and commercial. It may have a positive impact on cross-border litigation involving terrorist cases and the security industry by allowing and facilitating the taking of evidence.

3.5.5. **Decision 2001/470/EC on a European Judicial Network**

3.5.5.1. **Brief summary of the regime**

Decision 2001/470/EC\(^{167}\) (“Brussels II Regulation”) establishes a European Judicial Network\(^{168}\) in civil and commercial matters to facilitate cooperation between Member States and effective access to justice by providing information on Community and international judicial cooperation instruments. This includes activities to ensure the “smooth operation of procedures having a cross-border impact” and the “effective and practical application of Community instruments” (Decision 2001/470/EC, Art 3).

Decision 2001/470/EC also requires Member States to set up a contact point to meet the information and cooperation obligations of that Decision (Decision 2001/470/EC, Arts 5 and following). They are also responsible to respond to requests for judicial cooperation within 15 days of receipt (Decision 2001/470/EC, Art 8) and meet regularly to exchange information and experience (Decision 2001/470/EC, Art 10).

3.5.5.2. **Applicability in time**


3.5.5.3. **Conclusions Decision 2001/470 and relevance to the security industry**

The Decision 2001/470/EC establishes a European Judicial Network in civil and commercial matters to facilitate cooperation between Member States and effective access to justice. It may have an impact on cross-border litigation involving terrorist cases and the security industry by making cooperation between Member States smoother.

3.5.6. **Regulation 861/2007 on a European small claims procedure**

3.5.6.1. **Brief summary of the regime**

Regulation 861/2007 on a European small claims procedure\(^{169}\) (“Small Claims Regulation”) provides a procedure provides a simplified and accelerated procedure to handle cross-border small claims in civil and commercial matters. No lawyer is required for such procedure (Small Claims Regulation, Art 10). Small claims are limited to €2,000 maximum, excluding interest, expenses and disbursements (Small Claims Regulation, Art 2(1)).

A judgment on a small claim is enforceable notwithstanding appeal (Small Claims Regulation, Art 15(1)). A court may refuse to enforce a judgment on a small claim in limited case, including if the judgment is irreconcilable with an earlier judgment between the same parties in the same cause of action (Small Claims Regulation, Art 22).

---


The defendant has the right to request the court that gave a judgment to review it, for example if service was not effected in time for him to prepare his/her defence or if he/she was prevented from objecting due to force majeure (Small Claims Regulation, Art 18).

Member States must decide to allow appeal against a judgment on a small claim and, if so, the applicable procedure.

3.5.6.2. Applicability in time

The Small Claims Regulation entered into force on 1 August 2007 and its main rules applied from 1 January 2009.

3.5.6.3. Conclusions Regulation 861/2007 and relevance to the security industry

The Small Claims Regulation provides a simplified and expedited procedure to settle small claims in cross-border civil and commercial matters. Damage caused by an act of terrorism is likely to exceed the ceiling of €2,000; this procedure is thus not very relevant for the purpose of this study.

3.5.7. Regulation 1896/2006 on a European order for payment procedure

3.5.7.1. Brief summary of the regime

Regulation 1896/2006 on a European order for payment procedure\(^{170}\) ("Order for Payment Regulation") requires Member States to establish a simple and fast procedure to issue a European order for payment of uncontested claims. Such procedure is provided for specific amounts that have fallen in civil and commercial matters and to issue a European order for payment (Order for Payment Regulation, Art 1).

The applicant must identify the parties and the claim in question and briefly set out the reasons underlying it (Order for Payment Regulation, Art 7(2)). If all relevant requirements are met, the competent court will issue a payment notification. At this point the court does not have to go through the procedure of examining the merits of the claim. The European order of payment must be issued within 30 days of the lodging of the application.

The debtor may file a statement of opposition that does not have to be motivated with the issuing court within 30 days from service (Order for Payment Regulation, Art 16). A right of review after this 30-day period is also granted to debtors in limited circumstances, including if the order for payment was wrongly issued.

All procedural issues not specifically dealt with in the RPP shall be governed by national law (Order for Payment Regulation, Art 26).

3.5.7.2. Applicability in time


3.5.7.3. Conclusions Regulation 1896/2006 and relevance to the security industry

The Order for Payment Regulation allows debtors to obtain a European order for payment in cross-border civil and commercial matters. Claims against the security industry in cases of terrorism, however, are likely to be fairly complex and contested. This Regulation is thus unlikely to apply.

3.5.8. Regulation 805/2004 on European enforcement order for uncontested claims

3.5.8.1. Brief summary of the regime

Regulation 805/2004 on a European enforcement order for uncontested claims\(^{171}\) ("Regulation 805/2004") requires Member States to establish a procedure to make a judgment on uncontested claims in civil and commercial matters and to certify the judgment as a European enforcement order (Regulation 805/2004, Art 6). A claim is uncontested if, for example, the debtor expressly agreed to it or never objected during the court proceedings (Regulation 805/2004, Art 3(1)).

The original procedure must meet certain minimum standards to be entitled to be subject to a European enforcement order (Regulation 805/2004, Arts 12-19). The law of the Member State where judgment is taken must also provide a right to the debtor to request the review the judgment in limited cases ( Regulation 805/2004, Art 19).

The creditor may request a court in a different Member State to enforce this European enforcement order (Regulation 805/2004, Art 20). The court must reject such enforcement if it is irreconcilable with an earlier judgment with the same cause of action and between the same parties (Regulation 805/2004, Art 21). No security or deposit may be required from the creditor as a condition to the enforceability of the European enforcement order (Regulation 805/2004, Art 20(3)).

3.5.8.2. Applicability in time


3.5.8.3. Conclusions Regulation 805/2004 and relevance to the security industry

Regulation 805/2004 allows for a European enforcement order for uncontested claims. Claims against the security industry in case of terrorisms, however, are likely to be fairly complex and contested. This Regulation is thus unlikely to apply.

3.5.9. Directive 2008/52/EC on mediation

3.5.9.1. Brief summary of the regime

Directive 2008/52/EC on mediation\(^{172}\) ("Mediation Directive") requires Member States to authorize courts to propose mediation in cross border civil commercial matters (Mediation Directive, Arts 1 and 5). Member States must encourage the quality of the mediation, for


example via code of conduct (Mediation Directive, Art 4). They must also allow for a procedure for the agreement to be made enforceable by a court or public authority, except if the content of the agreement is contrary to the law of the Member State where the request is made or that law does not provide for such enforceability (Mediation Directive, Art 6).

The Mediation Directive also protects the confidentiality of the mediation by limiting the possibility for mediators to be compelled to give evidence and judicial proceedings, for example in the case of overriding considerations of public policy (Mediation Directive, Art 7).

3.5.9.2. Applicability in time


3.5.9.3. Conclusions Mediation Directive and relevance to the security industry

The Mediation Directive partly harmonizes rules related mediation in cross-border civil and commercial disputes. It may encourage and facilitate cross-border litigation involving terrorist cases by allowing and facilitating mediation with responsible parties, which may include the security industry.

3.5.10. Directive 2003/8/EC on legal aid

3.5.10.1. Brief summary of the regime

Directive 2003/8/EC on legal aid173 (“Legal Aid Directive”) requires Member States to provide legal aid to persons who do not have sufficient resources in civil and commercial procedures (Legal Aid Directive, Arts 1-3). Legal aid may include the assistance of a lawyer or exemption from proceedings costs, including pre-litigation advice.

The procedure for granting legal aid must be transparent and decisions rejecting legal aid must be motivated and an appeal must be available (Legal Aid Directive, Arts 15).

3.5.10.2. Applicability in time

The Legal Aid Directive entered into force on 31 January 2003 and had to be transposed by 30 November 2004.

3.5.10.3. Conclusions Legal Aid Directive and relevance to the security industry

The Legal Aid Directive partly harmonizes rules related to legal aid in cross-border disputes. It may encourage and facilitate cross-border litigation involving terrorist cases by allowing and facilitating actions against responsible parties, which may include the security industry. Moreover, the Directive on Legal Aid may support meritorious claims to be brought. Hence,

legal aid can increase access to justice for victims and in that sense potentially increase the exposure to liability of the security industry.

3.5.11. Directive 2004/80/EC relating to compensation to crime victims

3.5.11.1. Brief summary of the regime

Directive 2004/80/EC relating to compensation to crime victims174 ("Compensation Directive") requires Member States to operate a compensation scheme for victims of violent intentional crime committed in their territory. This scheme is available to victims, regardless of their country of residence (Compensation Directive, Art 12). The amount to be paid must be fair and appropriate (Compensation Directive, Art 12).

To facilitate compensation in cross-border cases, victims are entitled to ask for assistance from the authority of the Member State in which they reside (Compensation Directive, Arts 1-6).

3.5.11.2. Applicability in time

The Compensation Directive entered into force on 26 August 2004 and had to be transposed by 1 June 2006.

3.5.11.3. Conclusions Compensation Directive and relevance to the security industry

The Compensation Directive significantly improves the compensation of crime victims, which includes victims of acts of terrorism. Because of the ease with which compensation can be claimed under the Directive, victims of acts of terrorism might favour this compensation rather than suing any party involved, including the security industry.

However, the rules for compensation, including the total amount of compensation, may still vary from Member State to Member State. The Compensation Directive does not provide any subrogation mechanism that would allow the Member State to claim reimbursement against a responsible party, which could include the security industry. The availability of such subrogation right should be assessed based on the applicable law, as determined under the Brussels I Regulation (see above).

3.5.12. Regulation 593/2008 on the law applicable to contractual obligations (Rome I)

3.5.12.1. Brief summary of the regime

Regulation 593/2008175 ("Rome I Regulation") establishes rules to resolve conflicts of laws in civil and commercial contractual matters.

The Rome I Regulation recognizes the freedom of contractual parties to choose the law applicable to their contracts (Rome I Regulation, Art 3), with limited exceptions, such as consumer contracts. The choice of law must be express or clearly demonstrated by the terms of the contract or the circumstances of the case.

In the absence of choice of law, the Rome I Regulation provides default rules, including (Rome I Regulation, Art 3):

- a contract for the sale of goods or services shall be governed by the law of the country where the seller or service provider has his habitual residence;
- where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than the country indicated in by following the previous point, the law of that other country shall apply;
- where the law applicable cannot be determined pursuant to points 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected.

The Rome I Regulation provides that the law selected based on these rules must be applied even if it is not the law of a Member State (Rome I Regulation, Art 2). The security industry may thus face applicable laws from any country in the world.

The Rome I Regulation also regulates the burden of proof and presumption of law and provides that these are to be determined based on the law governing a contractual obligation (Rome I Regulation, Art 18(1)).

If there are multiple liable persons and one of them satisfied the claim in whole or in part, the Rome I Regulation provides that the law governing the payer’s right to claim recourse from the other debtors is the same as the law governing the payer’s obligation towards the creditor (Rome I Regulation, Art 16). A similar rule applies to contractual obligations under the Rome II Regulation (see report below). This provision would thus, arguably, apply to a situation where a creditor would have a contractual claim against a debtor (e.g., an airline) and a claim based on tort law against another one (e.g., a provider of security products or services).

3.5.12.2. Applicability in time

The Rome I Regulation replaces the Rome I Convention\(^{176}\) between the Member States.

The Rome I Regulation entered into force on 24 July 2008 and applies to contracts concluded after 17 June 2009.

3.5.12.3. Conclusions Rome I Regulation and relevance to the security industry

The Rome I Regulation harmonizes rules applicable to conflicts of law in contractual matters. It is thus applicable to contracts between the security industry and their customers.

The Rome I Regulation allows contractual parties to select a governing law that is either in favour of or disadvantageous to the security company involved. It also facilitates cross-border litigation and thus, indirectly, expands liability exposure. A clear regime for establishing the applicable law saves time and transaction costs.\(^{177}\)

\(^{176}\) Convention on the Law Applicable to Contractual Obligations 1980 (the “Rome Convention”).

\(^{177}\) See also Max Planck Institute for Comparative and International Private Law, Comments on the European Commission’s Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)” (2007), available at http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2612&context=faculty_scholarship&sei-redir=1&referer=http%3A%2F%2Fwww.google.be%2Furl%3Fsa%3Df%26rct%3Dj%26q%3Darticle%25205%2520rome%2520law%26t%3Dweb%26cd%3D3%26cad%3Drja%26ved%3D0CD
3.5.13. **Regulation 864/2007 on the law applicable to non-contractual obligations (Rome II)**

3.5.13.1. **Brief summary of the regime**

Regulation 864/2007 ("Rome II Regulation") establishes rules to resolve conflicts of laws in relation to non-contractual obligations in civil and commercial matters, such as damages caused by tort or *culpa in contrahendo* (Rome II Regulation, Art 2(1)).

In the absence of choice of law by the parties (Rome II Regulation, Art 14), the Rome II Regulation provides default rules, including (Rome II Regulation, Arts 4-12):

4) **product liability:** In order of priority,
   - the law of the country where the victim had his or her habitual residence when the damage occurred, if the product was marketed in that country;
   - the law of the country of acquisition, if the product was marketed in that country; or
   - the law of the country in which the damage occurred, if the product was marketed in that country.

If the defendant could not reasonably foresee the marketing of its product, or similar products, in that country, the applicable law must be the law of the country in which that defendant is habitually resident.

However, these rules will be overruled and a different law will apply, if the law of that country has a “manifestly closer connection” to the tort (Rome II Regulation, Art 5(2)).

5) The law applicable to environmental damages is the law of the country in which the damage occurred, unless the plaintiff chooses the law of the country in which the event occurred.

6) In other tort cases, the applicable law will be the law of the country in which the damage occurred, unless both plaintiffs and defendants have their habitual residence in the same country at the time the damage occurred or another country has a “manifestly closer connection” to the tort, in which case the law of that country applies (Rome II Regulation, Art 4(2) and (3)).

The Rome II Regulation provides that the law selected based on these rules must be applied even if it is not the law of a Member State (Rome II Regulation, Art 3). The security industry may thus face applicable laws from any country in the world.

The Rome II Regulation also regulates the burden of proof and presumption of law and provides that these are to be determined based on the law governing a contractual obligation (Rome I Regulation, Art 22(1)).

If there are multiple liable persons and one of them satisfied the claim in whole or in part, the Rome II Regulation provides that the law governing the payer’s right to claim recourse from

---

8QFja%26url%3Dhttp%253A%252F%252Fscholarship.law.duke.edu%252Fcgi%252Fviewcontent.cgi%252Farticle%252F253A%252F252Fscholarship.law.duke.edu%252F252Fviewcontent.cgi%252F253Fac ticle%2525D2612%2525D26context%2525D26faculty_scholarship%2526e%3D3DbLLMUOyuHaS1QHotoCQA%26usg%3 DAFQjCNE9sk9fP9HFMi8ydAeOoNi%26bvm%26Dvb.1355325884%2Cd.m#search=%22article%20regulatio n%20airlines%22> accessed on 15 December 2012

the other debtors is the same as the law governing the payer’s obligation towards the creditor (Rome II Regulation, Art 20). A similar rule applies to contractual obligations under the Rome I Regulation (see report above). This provision would thus, arguably, apply to a situation where a creditor would have a contractual claim against a debtor (e.g., an airline) and a claim based on tort law against another one (e.g., a provider of security products or services).

If a third person has a duty to satisfy the creditor, the law applicable to that obligation will also govern whether and to what extent the third person is subrogated in the rights of the creditors against the debtors (Rome II Regulation, Art 19).

The Rome II Regulation also provides a direct right of recourse to the victim against the insurer if this is provided by either the law applicable to the non-contractual obligation or the law applicable to the insurance contract (Rome II Regulation, Art 18).

3.5.13.2. Applicability in time

The Rome II Regulation entered into force on 11 January 2009 and applies to events giving rise to damage occurring after that date.

3.5.13.3. Conclusions Rome II Regulation and relevance to the security industry

The Rome II Regulation harmonizes rules applicable to conflicts of law in non-contractual matters. It is thus applicable to claims from victims against the security industry.

The Rome II Regulation allows parties to select a governing law that is either in favour of or disadvantageous to the security company involved. It also facilitates cross-border litigation which, indirectly, expands the security industry’s liability exposure as a matter of fact. A clear regime for establishing the applicable law can further save time and transaction costs.

The place where the damage occurred can be totally unpredictable in the case of a terrorist act involving means of transportation (e.g., airplane), which may make it difficult for the security industry to determine in advance which law will apply.

The different rules applicable to tort and product liability may also raise particular difficulties if they have to be applied jointly, for example, if the victim sues both the manufacturer of a weapon detector (under product liability law) and a service provider (under general civil liability or tort law).

3.6. Concluding observations

After the analysis of comparable EU legislation and related case law it may be useful to relate this back to the central question of this study, i.e. what a potential scope of liability for the security industry could be and to what extent related EU legislation provides interesting insights in that respect. Below, we will first summarize the results of the liability regimes by putting them into a schedule (3.6.1); next we will briefly look at the main results of the regulatory regimes (3.6.2) and then ask the question to what extent the current regimes as we analysed them can be applied to the security industry (3.6.3). The other key question in this research was to what extent the comparable EU legislation we analysed could provide interesting lessons for a possible future liability regime for the security industry. That will be analysed in 3.6.4.
3.6.1. Liability regimes

This chapter discussed EU liability regimes of particular relevance to the third party liability of the security industry, being the Environmental Liability Directive, the Product Liability Directive and the Recommendation concerning the limitation of the civil liability of auditors. Comparing these three regimes on the basis of the common format for the analysis of liability regimes, we can summarize this as follows.\(^{179}\)

Scheme 1: Comparison of liability regimes in comparable EU legislation

<table>
<thead>
<tr>
<th>Criterion basis</th>
<th>ELD</th>
<th>PLD</th>
<th>Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liable persons</td>
<td>Operator</td>
<td>Producers + importers</td>
<td>Accounting network</td>
</tr>
<tr>
<td>Damage</td>
<td>Heads of damage limited, but no financial cap</td>
<td>Limited to personal injury + private goods; optional cap</td>
<td>Three options for financial cap + optional introduction</td>
</tr>
<tr>
<td>Exclusions</td>
<td>Optional permit defence + state of the art defence</td>
<td>Development risk defence (but can optionally be excluded)</td>
<td>-</td>
</tr>
<tr>
<td>Causation</td>
<td>Determined by MS</td>
<td>Determined by MS</td>
<td>Determined by MS</td>
</tr>
<tr>
<td>Relation with regulation</td>
<td>-</td>
<td>Compliance does not shield, but may make product not defective</td>
<td>Link with audit directive</td>
</tr>
<tr>
<td>Financial security</td>
<td>Recommended to MS, mandatory in some MS</td>
<td>Not mandatory, but often used in practice</td>
<td>Expected positive impact on insurability</td>
</tr>
</tbody>
</table>

These liability regimes hence all have interesting features which may provide some source of inspiration for a possible liability regime for the European security industry. Some of those features will be further addressed below.\(^{180}\)

3.6.2. Regulatory regimes

Many of the regimes we examined in this chapter of comparable EU legislation did not concern real liability law;\(^{181}\) many were regulatory regimes which were nevertheless interesting to analyse. Indeed, with respect to most of the regulatory regimes the reason for analysing them was especially their relationship with liability law. For almost all regulatory regimes\(^{182}\) we came to similar conclusions as far as the relation with liability is concerned. Most of these regulatory regimes in some way or another impose regulatory requirements upon operators aiming at increasing safety. The question we addressed was whether the existence of such a regulatory regime could affect the liability exposure of operators. We made clear that the existence of a regulatory scheme always works like the well-known double-edged sword. On the one hand the existence of a regulatory regime can expand the liability exposure:

---

\(^{179}\) Not all aspects of the common format for analysis of liability regimes will be addressed since as far as the last two are concerned (rules of evidence and jurisdictional and procedural issues) the three liability regimes we examined did not have specific rules worth mentioning.

\(^{180}\) In section 3.6.4.

\(^{181}\) In fact the truly liability oriented regimes were in fact, as we showed, limited to three: environmental, product’s and auditor’s liability.

\(^{182}\) More particularly the General Product Safety Directive in 3.2.2.5, REACH in 3.2.3.5, the Plant Protection Product Regulation in 3.2.4.5, EURALEX in 3.2.5.5, the Personal Protective Equipment Directive in 3.2.6.5, the Machinery Directive in 3.2.7.5 and the Construction Products Regulation in 3.2.8.5.
especially where applicable standards are very stringent and exceed standards that otherwise would be applied under general civil law;
- generally, the regulatory regimes we discussed establish detailed safety standards and impose certain disclosure of information that can be used by plaintiffs to assess whether a product is safe;
- non-compliance with regulatory standards may constitute a breach of obligation of negligence per se which may trigger liability exposure. In that sense regulation may make the task of victims easier by showing a violation of a regulatory standard and could thus increase liability exposure.

On the other hand compliance with a regulatory regime could also limit liability exposure if:

- the regulation provides incentives to operators towards compliance, thus avoiding or limiting any risk of non-compliance and thus of liability exposure;
- a product that meets the requirements of the regulatory standard or certification may be regarded as “safe” or, within the framework of the PLD, as not “defective”. Even though we argued that compliance with regulatory standards will not preclude potential civil liability exposure compliance with regulation may be an important factor when considering liability of the operator.

Specific regulatory regimes also had interesting features that were discussed in detail, some of which we will examine further below. For example the Medicinal Code in the EUDRALEX regime provides explicitly that companies must not be subject to civil or administrative liability for unapproved use of medicinal products if such use is recommended or required by the authorities to address a suspected or confirmed public health problem. Here a parallel with the security industry could be made if authorities recommend the use of particular security products to address a suspected or confirmed security problem.

3.6.3. Relevance for the security industry

We will now briefly summarize to what extent the various regimes we examined in this chapter could be applied to the security industry, defined as above in Chapter 2. Hence we more particularly focus on the relevance for terrorism or organised crime. Potentially any type of legislation could be relevant for the security industry, but in that case an interpretation would in some cases be rather far-fetched. We therefore focussed on legislative regimes which are of more direct interest for the security industry.

Addressing first the liability regimes, the Environmental Liability Directive is an example of a regime where only if one would stretch its interpretation very far a relationship with the security industry could be seen.\(^\text{183}\) Therefore, we concluded that the ELD is not relevant for the security industry’s third party liability. The Product Liability Directive, on the other hand, certainly is. We note that security products could be deemed defective if they do not provide the security that the public in that particular case may expect. Questions still arise as to how one would have to interpret the public’s expectations in that particular case. Interestingly, the heads of damages covered under the PLD are limited to personal injury and private property intended for consumption and used by the victim for its own private use or consumption. Under the PLD, there is hence no liability for pain and suffering, nor for damage just to

\(^{183}\) If one were for example to assume that through negligence of a security provider a terrorist would cause an accident which would lead to environmental harm in the sense of the Environmental Liability Directive. However, even in that hypothetical case it is doubtful that the ELD would apply since the security industry would normally not be qualified as an operator in the sense of the ELD. Liability may, however, theoretically be possible under national law of some Member States.
professional property or for pure economic loss. The PLD moreover provides for an optional liability cap. The PLD excludes development risks which may be quite important for the security industry given large uncertainties on techniques used e.g. by terrorists. However, security providers do not have full security since Member States have the option of excluding the development risk defence. Compliance with regulation, such as REACH, may have an influence on liability in the sense that a product is no longer considered defective if it complies with regulation. However, this is not a necessary result. National courts may still consider a product defective and hence a producer liable notwithstanding compliance with safety regulation.

Interesting lessons can certainly be drawn from the recommendation concerning auditor’s liability. This, of course, is not directly applicable to the security industry, but the way in which auditors have been protected through the recommendation is an interesting example of how such a protection against increasing liability could be constructed.

Another piece of EU legislation with indirect relevance to the security industry is the regulation on insurance requirements for air carriers and aircraft operators. Although not directly applicable to the security industry, the regulation imposes mandatory insurance for aircraft carriers and aircraft operators to cover their potential liability. This may have a strong effect of channelling (in an economic sense) liability to air carriers and aircraft operators. Victims may have incentives to sue aircraft carriers and aircraft operators whose solvency is guaranteed through the mandatory insurance and which may hence reduce their incentives to sue the security industry. Potentially, this could thus limit liability exposure of the security industry.

In addition to addressing liability regimes also many regulatory regimes were discussed, some of which in fact have no relevance for the security industry whatsoever. This is the case, so we concluded, for REACH, for the Plant Protection Product Regulation, and for EUDRALEX. However, some other regulatory regimes do have some relevance for the security industry. This is, for example, the case for the General Product Safety Directive since compliance with this Directive could (although this will very much depend on the interpretation by the national judges in a liability setting) imply that the product is not defective and hence that the producer is not liable. Also the Personal Protective Equipment Directive does have some relevance for the security industry since this equipment is used by the security industry and compliance with the Directive may result in a higher level of safety for users, thus potentially limiting (or, as we mentioned expanding) liability. We reached the same conclusion for the Machinery Directive which can apply to security products that have a drive system. The same is the case for the Construction Products Regulation which equally applies to some security products that are incorporated in buildings. Again,
compliance with the imposed standards and post-marketing obligations could possibly result in a limitation of liability. 193

Finally, we should mention that all of the instruments of EU legislation we discussed in section 3.5 may facilitate access to justice for victims and to some extent increase the actual liability exposure of the security industry. This is, for example, the case with many of the regulations concerning jurisdiction and recognition and enforcement of judgments in various matters as well as for regulations on the service of judicial and extra-judicial documents on the taking of evidence and on mediation. They may all encourage and facilitate cross-border litigation and hence facilitate access to justice for victims.

3.6.4. Lessons for a future liability regime for the European security industry?

The question also has to be addressed whether the analysis of comparable EU legislation performed in this chapter can provide some lessons for a potential EU liability regime for the security industry. Various legislative instruments we examined present interesting features that are definitely worth further analysis. At this stage, we can only mention those without assessing these particular features normatively. Indeed, the mere fact that for example a particular legislative instrument would have an optional financial limit or a ‘compliance with permit’ defence does not necessarily mean that those would be desirable instruments to be applied to the EU security industry as well. In order to analyse that, a further (also economic) analysis of the pros and cons of various options will be presented in Chapter 8 when addressing legal and technical options for implementing a feasible third party liability regime in the EU.

When first addressing the attribution of liability, it is striking that the ELD channels the liability exclusively to the operator, thus potentially limiting liability of other parties who could contribute to environmental harm. The system of allocation of liability in the PLD is more complex, in principle allocating liability to the manufacturer or importer, but also expanding to the supplier of a product if the first two are unknown. In case of auditor’s liability, joint and several liability is recommended not only for individual audit firms or accountants, but also for accounting networks who could (depending on the legal system) be held vicariously liable. Already this point shows how the attribution of liability can have an important bearing on the scope of liability of the security industry. A regime which would e.g. for airport related security risks channel liability to air carriers and aircraft operators would thus exclude the liability of the security industry. A joint and several liability regime, to the contrary, would increase liability exposure of the security industry.

Also the scope of damages has an important bearing on liability exposure. This is not only the case for the (financial) limit on liability, but also for the heads of damages compensated. The ELD has no financial cap; the PLD does not have a financial limit either, but included the option for Member States to adopt a liability cap. Such an optional system is also provided for in the recommendation concerning audit liability which basically provides three options to Member States if they wish to limit auditor’s liability. The damages under the ELD are limited to damage to protected species, habitats, water damage and land damage, but traditional damage, such as damage to health and property, has been excluded. Also the damage covered in the ELD is limited to personal injury and damage to private property; other heads of damages are excluded. This may be an important issue since the literature, for example, with respect to auditor’s liability, held that especially economic losses and wrong assessment of damages were important reasons for a large liability exposure of auditors.

193 See 3.2.8.9.
The ELD has optional compliance with permit and state of the art defences, whereas the PLD excludes liability for development risks, but provides Member States the option to make producers nevertheless liable for development risks too. Whether it is desirable to hold the security industry liable for the development risk or not is an issue which will have to be discussed further, in the light of general goals of liability of the security industry. The question that will *inter alia* have to be addressed in that respect is to what extent liability for the development risk provides (additional) incentives to the security industry to invest in research and development.

An important aspect related to liability is whether it is covered by insurance. Especially when strict liability is introduced (such as in the ELD for Annex III activities as well as in the PLD for product defects) it is held that it is important to provide a financial guarantee against insolvency of operators. The ELD has no compulsory insurance requirement, but at least stimulates Member States to take measures to encourage the development of financial security instruments. The PLD completely lacks solvency guarantees. Interestingly, in some of the regulatory regimes discussed compulsory insurance was required, such as in the Machine Directive, as well as in the Construction Products Regulation. An interesting aspect of the Regulation on insurance requirements for air carriers and aircraft operators is that in case of insurance market failure, the Commission may determine the appropriate measures to realise the obligation of providing insurance coverage. Here, the limits of the insurance market in providing security are recognised and the Commission sees an active role for itself in determining appropriate measures to realise the obligation of providing insurance coverage.

An important aspect bearing on the scope of liability is the relationship to regulation. We already mentioned that the existence of a regulatory regime could have an important influence on liability. Of course, compliance with regulation (such as REACH) may not automatically exclude liability, but compliance could lead to a presumption of products being not defective. We already mentioned the example of EUDRALEX which explicitly holds that regulated entities must not be subject to civil or administrative liability for unapproved use of medicinal products if such use is recommended or required by the authorities in response to particular public health risks. Also, compliance with the personal protective equipment may lead to an assumption of conformity with basic safety requirements thus potentially reducing liability. Also the example of CE-marking directives, such as the Machinery Directive, is interesting where standards and certification could possibly result in a limitation of liability and where on the other hand machinery specially designed and constructed for police purposes is excluded from the scope of the Machinery Directive.

It merits further analysis what this precisely means. One has to be careful with drawing from this e.g. the conclusion that safety regulation of the security industry would be indicated. All depends on other factors, including the contents and quality of the regulation. For example, there is criticism of REACH holding that it would provide limited incentives for innovation. Moreover, it is one thing to take into account compliance with regulation as a presumption of following the due care standard or assuming “safety” of a particular product; it is quite another to infer from compliance with regulation that the security industry could not

---

194 See 3.2.7.6.
195 See 3.2.8.6.
196 See 3.3.6.
197 See 3.2.5.5.
198 See 3.2.6.9.
199 See 3.2.7.9.
200 See 3.2.3.9.
be held liable at all anymore. Hence, this relationship between regulation and liability still merits further analysis, also from the perspective of the economic analysis of law.

A final point, especially as far as potential EU action is concerned, is that one notices that the instruments analysed in this chapter often provide a lot of options for Member States. For example, the ELD leaves the important issue (having a significant influence on the scope of liability) of the compliance with permit defence to Member States and the same is true for the PLD which, for example, allows Member States to reject the development risk defence. The recommendation on auditor’s liability even goes a step further by providing Member States three options of (financially) limiting auditor’s liability. This way of regulating liability has the major advantage of providing a lot of flexibility and leaving it largely up to the Member State to determine the scope of liability, thus respecting the subsidiarity principle and having the benefits of flexibility and differentiation. However, for an industry branch where risks are typically transnational (like the security industry) operators working in this transnational branch may wish to have a European-wide liability regime in order to create an EU-wide level playing field. This is again a trade-off that needs further attention.

Also it is important to stress that one particular issue which has an influence on the potential liability of the security industry is in fact not explicitly regulated in any of the EU legislation discussed in this chapter. The topic we refer to is causation. This is a crucial issue since the security industry will normally never be considered itself a direct tortfeasor or injurer. The direct tortfeasor will often be a criminal organisation or terrorists who intentionally inflict harm on victims. The charge against the security industry may be that through its negligence it facilitated the terrorist activity that inflicted harm upon the victims. The extent to which one accepts liability of the security industry in that case is strongly related to the question whether one considers the behaviour of the security industry (supposedly wrongful) as a cause of the damage suffered by the victims. Notions like the proximity of the cause, breaking the chain of causation, and the remoteness of damage are hence crucial in that respect. These issues are not dealt with explicitly in any of the EU legislation analysed in this chapter, but do have a crucial bearing on the scope of liability of the security industry. Causation will, however, be analysed in detail in the analysis of Member States legislation, which is the focus of the next chapter.
Chapter 4 Analysis of comparable EU-Member States legislation and related case law

4.1. Introduction

This chapter aims to address the current situation in the national legal systems of 7 EU Member States: England and Wales, France, Germany, The Netherlands, Poland, Spain and Sweden.

The reporters were asked to answer a detailed questionnaire covering the relevant features of national tort law and five cases in which the special liability situation of the security industry is explored. The reporters were asked to indicate any unique features of the relevant rules in their national system and also to reflect how the burden of the various risks contained in and created by the security industry is divided between whatever different liability, regulatory or alternative compensation regimes exist in their system. The reports reflect both the black-letter law that applies to the security industry and also how that liability is contextualised and influenced by other national regulatory or public law regimes. Further attention had to be given to the extent to which the various applicable EU regimes have been interpreted.

The questionnaire was drafted by Monika Hinteregger. She is also responsible for the comparison and the conclusions for the security industry. Helmut Koziol (European Centre of Tort and Insurance Law, Vienna) and Ken Oliphant (Institute for European Tort law, Vienna) reviewed the national submissions and commented upon the questionnaire and the comparative conclusions. The national reporters are:
- England and Wales: Claire Mc Ivor, University of Birmingham
- France: Florence G’sell Macrez, Université de Bretagne Occidentale
- Germany: Peter Rott, University of Copenhagen
- Netherlands: Siewert Lindenbergh, Willem van Boom, Erasmus University Rotterdam
- Poland: Ewa Baginska, Nicolaus Copernicus University, Torun
- Spain: Pedro del Olmo, University Carlos III of Madrid
- Sweden: Philip Mielnicki, Marten Schultz, Stockholm University

These countries cover the major national markets for security related products and services in Europe. The further aim of the selection was to ensure a good mix of common law and civil law systems and to include representatives of the major legal families (common law, Germanic, Romanic and Nordic law). With the addition of Poland, one major jurisdiction of the new democracies of Eastern and Central Europe is also represented.

4.2. The Questionnaire

A. General Questions

This section of the questionnaire is aimed at presenting the application of the black-letter legal rules to the Security Industry. So as to avoid an overly generalized summary of the national rules (i.e. a textbook approach), please try to keep the focus of examples and explanations on situations which are relevant to the Security Industry. Please indicate all cases or court decisions that relate to the Security Industry.

---

201 This corresponds to Work Package 2 of the Invitation to Tender.
I. Bases of liability

1. Fault based liability

a) Please describe very briefly the fundamentals of fault based liability in your jurisdiction. The analysis should include:

- assessment of fault,
- effects of contributory fault,
- burden of proof in general (standard of proof) with respect to the proof of fault
- availability of instruments to lighten the burden of proof for the claimant (reversals, presumptions etc.) with respect to the proof of fault,
- vicarious liability (Gehilfenhaftung),

b) Are there special rules with respect to the concurrence of contractual and non-contractual claims?

2. Product liability

Do the product liability rules in your jurisdiction differ from the EU-Products Liability Directive? Please describe the differences.

3. Special liability regimes

The aim of this section is to highlight and examine in detail a number of specific sectors, actors and issues that are known to be problematic in relation to the Security Industry.

a) Does your jurisdiction provide for instruments to tighten or increase liability with respect to dangerous activities (e.g. alterations to the burden of proof for fault or causation)?

b) Does your jurisdiction provide for special rules concerning third party liability for airplanes, genetically modified organisms, nuclear installations, medical products (pharmaceuticals) and environmental harm? Please describe them (examples would include the availability of strict liability, alterations to the requirements for proof of causation, compensable damage, liability caps, defences).

II. Relationship with regulation

1. Please explain the relationship of tort liability with regulations (consequences of compliance with regulations and consequences of breach of legal rules).
2. Are there specific regulations governing the risks of the Security Industry? How and by which regulatory body are these rules enforced?

III. Causation

1. What is the burden of proof in general (standard of proof) with respect to the proof of causation?
2. Does your jurisdiction provide for any instruments to lighten the burden of proof for the claimant (reversals, presumptions etc.) with respect to the proof of causation?

IV. Attribution of liability

1. How is liability attributed to multiple parties (proportional or joint and several liability, recourse against contributors)?
2. Does your jurisdiction - in fault-based or no-fault liability - provide for the (legal) channelling of liability to one person (e.g. the operator of a dangerous activity)?
V. Damages and available remedies

1. What types of compensable damage are available
   a. pecuniary loss,
   b. non pecuniary loss (pain and suffering),
   c. pure economic loss,
   d. environmental damage.
2. Are there particular heads of damage that can be excluded by contractual agreement or
   by any other means?
3. Does your jurisdiction - in fault-based or no-fault liability - provide for instruments
   which mitigate the liability of tortfeasors, such as liability caps or reduction clauses?

VI. Applicability in time

Does your jurisdiction allow the introduction of a new liability regime that also covers risks
that were created in the past (retroactive or retrospective liability)?

VII. Alternative compensation mechanisms

1. Are there alternative compensation schemes available for particular sectors
   a. compulsory liability insurance or other duties to seek financial coverage for
      liability,
   b. mandatory or voluntary first party or direct insurance schemes,
   c. risk sharing agreements or pooling schemes between operators,
   d. ex ante guarantees and deposits of a voluntary or mandatory nature?
2. How do these operate (size, scope, recovery, usage)?
3. What harm is covered by any applicable scheme?
4. Is there a cap on the amount recoverable under any applicable scheme?
5. What sorts of damages are covered by the social security mechanisms and what is the
   level of compensation?
6. Does civil procedure law provide for special rules on case management (joining of
   actions etc)?

VIII. Suggested reforms in national literature

Please outline in brief, any suggestions for reform that exists in the relevant literature or law
reform bodies (Law Commission, Ministry of Justice etc) as it applies to the liability of the
Security Industry. Please indicate whether a suggested development is aimed at solving
specific problems concerning the liability of the security industry and indicate the advantages
of such a suggested approach over the status quo.

IX. Successes and failures of the national approach

Please give an assessment of the national rules governing the liability of the Security Industry.
Do you see any innovative concepts or any flaws?

B. Cases

Please give analyses from the perspective of your jurisdiction of the following cases. You
may of course rely on cross references to your replies to the general questions above wherever
suitable.

Case 1
Defective emergency stop button
**Aim of the case:**
- to apply the national rules concerning fault based liability and liability for products (products liability or any other applicable strict liability)
- to describe the types of damage that are compensable (personal injury, property damage, pure economic loss) under these rules
- to explore the consequences of breach of technical standards or regulations for the liability of the producer of a technical device

Company X operates a steel plant. One year ago it bought a heavy stamping machine from Company A. While operating the machine, the worker sees that C, who is part of a group of visitors on a plant tour, is getting too close to the machine. B pushes the pilot trigger to stop the machine. The pilot trigger was built into the machine by A in order to allow the sudden stop of the machine by cutting the electricity supply. Due to a manufacturing defect the button fails to function and C gets injured.

a) Is A liable for C’s injury? Please describe all heads of liability that are applicable.
b) Is A liable to C if C has, by his own fault, contributed to the damage?
c) Would it make any difference if C had suffered property damage instead of personal injury?
d) Because of the incident, company X cannot operate the stamping machine for 14 days. Accordingly company X cannot fulfill the contract with Y in time. X has to pay Y € 200,000 for breach of contract. Is A liable to X for the loss?
e) Due to X’s failure to fulfill the contract Y has to renounce a profitable contract and suffers € 50,000 loss of profits. Is A liable to Y for this loss?
f) Would it make any difference whether the emergency stop button complies with the EN-standard issued by the European Committee for Standardization or not?
g) What is A’s liability like if the emergency stop button does not comply with a national standard provided by a legal provision (law or regulation)?

**Case 2**
Defective safety programmable logic controller

**Aim of the case:**
- to explore the liability for the rendition of services
- to explore the consequences of natural disasters for the liability
- to explain the principles of vicarious liability
- to explain attribution of liability in case of multiple tortfeasors

The computer firm A developed a special computer program for company B who runs a chemical plant. The computer program shall ensure that in case of an emergency the production process is ramped down in a controlled manner. On Monday 7 June a heavy earthquake shakes the region where the plant is situated. Due to a programming defect the production process is shut down immediately and as a consequence dangerous chemicals escape from the plant into the surroundings.

The local fire brigade C takes emergency measures to remove the chemicals from the water and to stop the chemicals from leaking into the nearby river. The costs of these relief measures for C amount to € 30,000. For fear of pollution of the groundwater, the local water supplier D employs tank wagons for the water supply of the local community for four weeks after the incident at the cost of € 70,000. On the adjoining land the chemicals leak into the groundwater. Neighbour E who uses the well on his land for the supply of drinking water suffers health damage. The removal of the chemicals from the well costs neighbour E € 50,000.
a) Are A or B, or both of them, liable for these costs? If B is liable, can B take recourse against A?
b) The computer program was especially designed for the prevention of pollution damage in case of natural disasters. The earth-quake from 7 June, however, was of an exceptional strength. Is A liable for the damage described in the case?
c) The flaw of the program was caused by the carelessness of the programmer F who is employed by A. Are A or F, or both of them, liable for the harm as described in the case? If A or F are liable, can they take recourse against the other party?
d) Due to the incident the nearby factory G is not able to fulfill its contracts and suffers a loss of € 40,000. Are A, B or F liable for this loss?
e) Assume that the cause of the incident is not an earthquake but instead a terrorist attack. The damage amounts to € 2.5 billions. Would there be a difference if the cause of the incident was an act of organised crime?

Case 3
Security services, public service (infrastructure) undertaking

Aim of the case:
- to explore liability of the renderer of security services
- to explore liability in case of a terrorist attack against a public service (infrastructure) undertaking and the recourse option of the public service undertaking against the renderer of security services

Company A is in charge of the operation of the security of the waterworks of city B. It provides manned guards to prevent unauthorised access to the plant and also operates the alarm systems of the plant. On 2 October terrorist C enters the plant and contaminates the water with radioactive material which is extremely poisonous (Polonium-210). Company A could have prevented terrorist C from entering the premises but failed to do so due to negligence. The consequences of the terrorist attack are disastrous (100 people are killed, 4,500 suffer from radiation sickness, the drinking water and the water supply system is contaminated). The total damage amounts to € 25 billions.

a) Is city B liable to the injured inhabitants (damage to person and property damage)? Can city B take recourse against A?
b) Is A directly liable to the house owner D who suffers property damage (€ 35,000) and severe health damage because of the contamination of the water?
c) Is A liable to state E who provides for disaster relief measures which amount to € 18 billion.

Case 4
Security services, border control

Aim of the case:
- to explore liability of the renderer of security services (security consultant, provider of security equipment) to the public authority
- to explore liability in case of public authority liability and the recourse option of the public authority against the renderer of security services

Company A is the security consultant of state B for border control security. A provided a comprehensive security concept for state B. It can be established that terrorist C of case 4 slipped through the border crossing point X of state B on 1 October. This was only possible because A’s security arrangements are seriously flawed.

a) Is state B liable to the house owner D of case 4?
b) Can state B take recourse against company A?
c) What would the liability of state B be like if company A was not a security consultant but rather the contractor who is obliged to service the video surveillance installation at the border crossing X, and terrorist C slipped through the border control because of A’s negligence?

Case 5
Security services, airplane-crash

Aim of the case:
- to explore liability of the renderer of security services
- to explore liability in case of airplane accidents and the recourse option of the air carrier against the renderer of security services

Company A is in charge of the security check at airport B. A’s obligations are determined in a contract with B which *inter alia* provides that A shall only use specially trained and certified personnel. On Sunday 2 April, employee C who lacks this special training is in charge of baggage screening monitor 5 at gate 25 of airport B. When passenger D is passing through the monitor employee C is chatting with another passenger and fails to detect that passenger D is carrying a box filled with highly inflammable chemicals in his hand baggage hidden under a notebook. Passenger D gets on the flight F-676 of airline E. In full flight the chemicals become inflamed and a fire starts in the passenger cabin. After some minutes the crew can stop the fire and manage an emergency landing at airport F. Five passengers suffer severe gas poisoning, two of them die and three have severe lung injuries. The airplane is heavily damaged. The repair costs amount to € 1.5 million. Air carrier E has to pay € 100,000 for the emergency landing to airport F, and the passengers of flight F-676 claim compensation for enduring fear of death and loss of profits.

a) Is A liable for these costs, if passenger D’s behaviour resulted from mere carelessness?
b) Is A liable for these costs, if passenger D acted with the intention to bring the aircraft down (terrorist attack)?
c) Is A liable if it can only be established that passenger D slipped through the security control? The exact reason is unclear. It is only possible that C was careless.
d) Passenger D is a terrorist. The crew cannot exterminate the fire, and the aircraft crashes into a residential area and causes disastrous damage to persons and property (€ 3.5 billion). All the passengers and the crew are dead. Is A liable for the damage? Is the aircraft carrier E liable for the damage? Can E take recourse against A?

4.3. Comparison

4.3.1. Bases of liability

4.3.1.1. Fault based liability

All the analysed jurisdictions provide for a sort of fault based liability. The preconditions for the attribution of liability are rather similar, but not identical. In the common law jurisdiction of England and Wales the most important head of liability is the tort of negligence, the tort most similar to the concept of fault based liability in civil law. In the civil law countries fault based liability is regulated in the civil codes. In Germany the basic provision is § 823 BGB (*Bürgerliches Gesetzbuch*) which provides for two heads of liability. According to § 823 (1) BGB, a person is liable who, intentionally or negligently, unlawfully injures the life, body,

---

202 Please note that the national reports are included in a separate document attached to this Final Report.
health, freedom, property or another right of another person. Under § 823 (2) BGB liability is provided for the intentional or negligent breach of a statutory duty. In the Netherlands fault based liability is defined in Article 6:162 BW (Burgerlijk Wetboek). In France, Poland and Spain the civil code provides for a general clause on fault liability. In Sweden it is a general rule, established by case law and legal doctrine, that liability requires fault. Since 1972 this rule is explicitly laid out in the Swedish Tort Liability Act (Skadeståndslag).

Duty of care and unlawfulness
The tort of negligence in England and Wales is comprised of four elements: actionable damage, duty of care, breach of duty and causation. For cases where it is not apparent that the defendant owed a duty of care to the claimant, courts developed the ‘Caparo test’. According to this test, a duty of care exists if the following requirements are met: foreseeability, proximity and, as a broad policy consideration, the requirement of fairness, justice and reasonableness. This test is applied when the existence of a duty of care is not apparent, for instance when the negligence claim relates to omissions, psychiatric harm or pure economic loss. For the provision of financial services a duty of care to third parties will generally only be established if the conditions of the Hedley Byrne test are met which requires, on the one hand, that the defendant voluntarily assumed responsibility to protect the financial interests of the claimant and, on the other hand, that the claimant reasonably relied on this act. Moreover, under English tort law there is no general duty to prevent damage to another. A duty to rescue is only recognised if there is some kind of special relationship of close proximity between the defendant and the claimant. Special duty of care obligations are imposed on manufacturers, designers, installers and repairers of products and on occupiers, who are obliged to take reasonable care to ensure that their product or property does not cause foreseeable physical injuries to another.

In the civil law countries an action under fault based liability must meet four requirements: actionable damage, unlawfulness, fault and causation. With respect to the criterion of unlawfulness, there is a basic difference between the Romanistic countries and the other jurisdictions. In the two Romanistic countries that are analysed in this study, France and Spain, the criterion of unlawfulness is not regarded as a separate requirement but is absorbed by the criterion of fault. The French reporter in particular showed quite clearly that in French law the assessment of fault includes deliberations which in German and Dutch law are made with respect to the criterion of unlawfulness. Fault is thus an unlawful conduct that violates an obligation or a duty imposed by law or custom or a general standard of behaviour. In Germany and the Netherlands the behaviour of a tortfeasor is regarded as unlawful if it infringes a protected subjective right of another (life, property, personality right etc) or if it violates a statutory duty. In the latter case it is necessary that the damage and the person who claims for the damage are within the protective scope of the infringed rule. Whether this is the case must be determined through interpretation of the rule. Dutch law recognises a further, more general category, the ‘maatschappelijke betamelijkheid’, according to which a behaviour which contravenes an agreed standard in society can be deemed unlawful.

Breach of duty of care and fault
While the criterion of unlawfulness relates to the assessment of the act of the tortfeasor, the prerequisite of fault deals with the blameworthiness of the concrete actor. The assessment of fault in the civil law countries meets the English concept of the ‘reasonable person’. In

203 Articles 1382 et seq French Civil code (Code Civil); Article 415 of the Polish civil code (Kodeks cywilny); Article 1902 of the Spanish civil code (Código Civil). In Spain, when damage was caused by a criminal act, liability is regulated by the criminal code (Código Penal) which provides for comparable rules.
204 Established in Caparo Industries Plc v Dickman [1990] 2 AC 605.
English law this standard results from the assessment of several factors including the magnitude of the risk, the gravity of the harm, the cost of precautions and the social utility of the defendant’s conduct. Many reporters stress that – except for children and disabled persons – the assessment of fault follows an objective (France) or predominantly objective standard (England and Wales, Germany, Netherlands). In all the jurisdictions specialists and professionals must meet a higher standard according to their special knowledge and abilities. In Spain there is even a tendency to align fault based liability with strict liability by raising the 'standard of care to levels which are almost impossible to achieve’.206

Contributory negligence
In all the analysed jurisdictions, contributory negligence of the claimant is a defence.207 For personal injury claims in Sweden this defence only applies if the behaviour of the claimant amounts to gross negligence or if he acted with intent. In all jurisdictions contributory negligence leads to a reduction of damages.

Vicarious liability
All jurisdictions provide for vicarious liability, but the concepts are quite different. In England and Wales vicarious liability covers not only employers who are liable for the misdemeanour of their employees in the course of their employment, but also relationships that are merely ‘akin to employment’, like the position of a priest in a church (see The Catholic Child Welfare Society v Various Claimants208). As reaffirmed by Lister v Hesley Hall209, vicarious liability includes intentional wrongdoing and takes a rather broad view of what constitutes the required ‘close connection’ between the behaviour of the employee and the employment. In case of loaned employees, even dual vicarious liability can be applied. The employer is entitled to bring an indemnity claim against the employee, but there is a tradition for such claims not to be enforced.210 The victim can also directly sue the employee. Vicarious liability also applies in French law provided that the employee acted within the course of the employment and the limits of his tasks. In this case the employee cannot be sued personally. Recourse by the employer against the employee is possible, but restricted to cases of gross negligence. Swedish law also provides for vicarious liability of the employer, but does not usually allow the employer to take recourse against the employee or the third party to sue the employee for damages. In the Netherlands Article 6:170 BW provides for vicarious liability for employers for the tortious acts committed by their employees. This extends not only to formal labour contracts, but also to other comparable relationships provided that there is a certain hierarchy between the principal and the agent. The employee can be directly sued by the victim, but the employer bears the full burden of liability unless the employee acted intentionally or with gross and wilful negligence (Article 6:170 (3) BW). Article 430 of the Polish Civil code has an equally broad concept of vicarious liability for employers and comparable persons. The employee cannot be directly sued by the victim, unless the employee acted with intent or the employer is insolvent or under-insured or the damage was not inflicted in the course of the employment (Article 120 Labour Code). In labour relations the recourse is limited to the equivalent of three months earnings of the employee unless the employee acted with intent. In Germany vicarious liability in non-contractual relationships is more restricted. According to § 831 BGB, the principal is liable for harm to third parties that is caused by an agent who is subjected to the principal’s authority. The agent must act unlawfully, albeit not necessarily with fault. The principal is exonerated if he proves that he

206 See Spanish report, 1.1.A.
210 See English report, Case 2 question c.
exercised reasonable care when selecting the agent or managing the activity or if the damage would have occurred even if this care had been exercised. Spanish law, however, does not provide for vicarious liability in the strict sense. Employees can be directly sued by the victim under fault-based liability. According to Article 1903 Código civil, employers are liable for damage caused by their employees for their own fault which however is presumed by law (culpa in eligendo and vigilando). This liability is strict, as courts in the past usually did not allow for the rebuttal of this presumption, although this seems to be changing now. The same applies correspondingly to parents and guardians for damage caused by minors or legally incompetent persons who are under their guardianship and to heads of schools for their underage pupils. Employer’s liability only applies to entrepreneurs and requires that the damage is caused by an employee in the course of the employment. Whether the employee must act negligently or not is still disputed. Recourse against the employee who has acted with fault is possible, but very uncommon. As Spanish law requires a hierarchical relationship between the principal and the agent, the principal is not responsible for the tortious act of an independent contractor unless the principal himself committed fault (culpa in eligendo or vigilando) or violated non-delegable duties. The same rule applies under Polish law where liability for the independent contractor requires fault on behalf of the principal (Article 429 Kodeks cywilny). The principal can be exonerated from liability if he proves either that he was not negligent in choosing the contractor (culpa in eligendo) or that he entrusted the performance of the activity to a professional, be it a person, enterprise or other institution. In the Netherlands Article 6:171 BW extends vicarious liability to cover the independent contractor if the contractor’s activity was actually, or at least in the perception of third parties, part of the client’s business. Germany and Sweden do not accept vicarious liability for the independent contractor in extra-contractual liability.

Burden of proof
In principle the burden for the proof of fault lies with the claimant in all the jurisdictions. In England and Wales there is no exception to this rule. Under certain conditions, however, the doctrine of res ipsa loquitur may be applied by which the breach of a duty of care is inferred from the fact that the thing that caused the damage was under the sole control of the defendant or his agent and that the accident is such that it would not normally happen in the absence of negligence. In many civil law countries (Germany, the Netherlands, Poland) a comparable instrument to lighten the burden of proof is concept of the prima facie evidence which plays an important role in medical malpractice cases.

For certain fields of liability or under certain conditions the burden of proof is shifted to the defendant. In Germany special rules apply for the burden of proof concerning vicarious liability in non-contractual relationships under § 831 BGB and in product liability cases. If the claimant can establish that the product is defective and that the defect caused the damage, the producer must show that he was not at fault. In the Netherlands Article 150 of the Dutch Code of Civil Procedure allows the court to reverse the burden of proof if this is stipulated by a special statute or if it is seen to be reasonable and fair. Polish law provides for a presumption of fault in cases of vicarious liability concerning liability for the independent contractor, minors and incapable persons. In France fault is assumed if a certain duty is imposed by a statute or by the courts. The defendant then can only escape liability in cases of force majeure or if he can show a ground of justification (eg self-defence). In Spain the courts are ready to infer the defendant’s fault from the fact that damage occurred or to attribute the burden of proof to the defendant based on the ‘theory of risk’ according to which the burden of proof lies with the person who profited from the introduction of a risk.

The required standard of proof varies in the jurisdictions analysed. The lowest standard of proof applies in England and Wales and the Netherlands where the relevant standard of proof is the balance of probabilities. German, Spanish and Swedish law require that facts are established with high probability, while in Poland the required level of probability is close to certainty (beyond reasonable doubt). French law does not deal with the notion of “standard of proof”
as such, but merely requires that fault must be established as provided by Articles 1315 and 1353 Code civil.

Concurrence of contractual and non-contractual claims
If contractual and non-contractual claims are available the claimant is free to choose either cause of action. The only exception is France, where the claimant who can rely on contractual liability is not allowed to invoke extra-contractual liability (principe de non cumul). Several reporters (Netherlands, Spain and Sweden) pointed out that the principle of concurrence of contractual and extra-contractual liability does not release from the obligation to observe the relationship between the extra-contractual and the concrete contractual duty which has important consequences for the right to sue for damages. This will be further outlined in 4.4.

4.3.1.2. Product liability

In all the jurisdictions analysed, product liability is regulated according to the Product Liability Directive\(^{211}\) (see chapter 3.2.1.), although many reporters stress that national courts still apply specific national product liability rules derived from fault based liability (England and Wales, France, Germany, Netherlands). Although the national laws implementing the Directive\(^ {212}\) follow the rules of the directive very closely, some deviations gave rise to infringement proceeding before the European Court of Justice. A prominent example is the English implementation of the ‘development risks’ defence of Article 7 (e) of the Directive\(^ {213}\) which prompted the European Commission to bring an infringement action against the UK according to Article 258 TFEU (ex-Article 226 TEC). The European Court of Justice admitted that there are some inconsistencies in the wording of the two provisions but nevertheless dismissed the application because it did not doubt that the courts in the United Kingdom would interpret section 4 (1) (e) Consumer Protection Act 1987 in the light of the wording and the purpose of the Directive.\(^ {214}\) With respect to France, which was already condemned in 1993 by the ECJ for not implementing the Directive,\(^ {215}\) the issues brought before the ECJ by the Commission were the inaccurate implementation of the liability of the supplier,\(^ {216}\) the broad definition of recoverable damage which also included property damage for the professional user of a product\(^ {217}\) and the non-implementation of the € 500 threshold for damage to property.\(^ {218}\)

In Poland the notion of the importer and the definition of the absolute prescription period deviate slightly from the rules of the Directive. According to Spanish law, the supplier who

---


\( ^{212} \) France: loi n° 98-389 du 19 mai 1998 which inserted the new section IV ‘de la responsabilité du fait des produits défectueux’ (C. civ., art. 1386-1 à 1386-18) into the Code civil; Germany: Produkthaftungsgesetz; Sweden: Produktansvarsvalg (1992:18); UK: Consumer Protection Act 1987; Poland: Article 449\(^ 1\)-449\(^ {10}\) civil code; Spain: Ley 23/1994 of 6 July 1994 de Responsabilidad Civil por los daños causados por productos defectuosos (LRPD) as revised by Royal Legislative Decree 1/2007 of 16 November 2007 por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLDCU).

\( ^{213} \) Section 4 (1) (e) Consumer Protection Act 1987.

\( ^{214} \) Case C-300/95 Commission of the European Communities v United Kingdom [1997] ECR I-2649.

\( ^{215} \) Case C-293/91 Commission of the European Communities v French Republic [1993] ECR I-1.

\( ^{216} \) Case C-52/00 Commission of the European Communities v French Republic [2002] ECR I-3827; Case C-177/04 Commission of the European Communities v French Republic [2006] ECR I-2461.


\( ^{218} \) Case C-52/00 Commission of the European Communities v French Republic [2002] ECR I-3827; Case C-183/00 María Victoria Gonzáles Sánches v Medicina Asturiana SA [2002] ECR I-3901.
markets a product despite having knowledge of a defect is liable to a third party as if he were the producer, from whom nonetheless, after having paid damages to the victim, he may seek recovery. In Spanish law the ‘reasonable’ period provided by Article 3 § 3 of the Directive for the supplier to identify the producer is three months. Slight deviations from the Directive also exist with respect to the prescription period.

All the analysed countries allow for the development risk defence as provided by Article 7 (e) of the Directive, except for certain products (France: products derived from the human body; Germany: pharmaceuticals; Spain: medicines, food or foodstuffs for human consumption) and, except for Spain, include the recovery of non-pecuniary damages.219 Germany and Spain provide for liability caps in case of death or personal injury (Germany: € 85 million; Spain: € 63,106,270.96).

4.3.1.3. Special liability regimes

4.3.1.3.1 General instruments to tighten or increase liability regarding dangerous activities

English law has no general strict liability regime for dangerous activities. With respect to damage caused by polluting interference the torts of public and private nuisance are applicable which do not require fault. While public nuisance provides for recovery for personal injuries and property damage as well as pure economic loss,220 private nuisance requires interference with a proprietary interest in land and covers only property damage. Moreover, the rule in Rylands v Fletcher,221 a sub-category of private nuisance, establishes a form of semi-strict liability governing property damage caused by the escape of dangerous things.

The French reporter stresses that the creation of a dangerous situation could itself constitute fault and give rise to liability. As the damage is often then easily foreseeable, it would also facilitate the proof of causation. The precautionary principle which enjoys constitutional protection under French law can also create specific obligations to prevent damage and thus influence the assessment of fault especially in cases of environmental harm. A very comprehensive and in practice very important no-fault liability is provided by Article 1384 (1) Code civil, according to which the custodian of a thing is responsible for the harm caused by the thing (‘responsabilité du fait des choses’). The thing need not be dangerous. According to Article 1384 (2) Code civil, an exception applies to the custodian of the thing, be it land or chattels, for damage to the neighbourhood caused by fire. In this case the victim has to prove fault on behalf of the custodian. Special rules amounting to strict liability apply for damage caused to the neighbourhood (‘troubles de voisinage’). Under this theory, the claimant must only prove an excessive level of the disturbance. The fact that the disturbance was abnormal can be induced from the excessive quality of the interference but also from the violation of regulation. Permissible objections include only fault of the victim and force majeure, which requires that the damage was caused by facts that came from outside and were of an unforeseeable and irresistible character. However, Article L 112-16 of the Code of Construction and Housing may restrict from a cause of action any plaintiff who only subsequently moved into the vicinity of an existing plant under certain conditions.

219 In German law compensation for pain and suffering was introduced into the Produkthaftungsgesetz only in 2001.
220 See English report, Case 2 question d.
221 (1866) LR 1 Ex 265.
German law does not provide for a general rule of no-fault liability for dangerous activities. There are, however, a number of statutory strict liability rules for specific activities, and under certain conditions courts are inclined to reverse the burden of proof for fault when damage is caused by a dangerous activity.

The Dutch reporter points out that even under fault-based liability the assessment of fault will be more stringent when damage is caused by an inherently dangerous activity. According to case law, dangerous activities can also elicit the reversal of proof concerning causation (‘omkeringsregel’). For the professional use or possession of dangerous substances the Dutch civil code provides a special strict liability regime that covers damage to person and property, but not pure economic loss (Articles 6:175 BW et seq). With respect to this head of liability a broad range of defences apply. Strict liability is further provided for defective objects (movables: Article 6:173 BW; immovables: Article 6:174 BW).

Polish law provides for several strict liability statutes for certain objects and dangerous activities (see below). According to Article 435 of the Polish civil code, the person who runs an undertaking set into motion by natural forces (steam, gas, electricity, liquid fuel etc) is liable for any damage to persons and property caused through the operation of the enterprise or business. The operator is not liable in cases of force majeure, or if he proves that the damage was caused exclusively through the fault of the injured party or of a third party for whom he is not responsible. A special no-fault liability applies to the organizer of a mass event (Article 5 of the Act of 20 March 2009 on mass events).

In Spain courts have started to impose strict liability on the operator of abnormally dangerous goods or activities, although this is not explicitly provided by law. Moreover, courts tend to tighten fault based liability under Article 1902 Código civil by reversing the burden of proof for the proof of fault.

Swedish law provides for a series of strict liability rules for dangerous activities covering the risks of airplanes, nuclear installations, railways and electricity providers as well as the causation of environmental harm or damage caused by oil spills from a sea vessel. Outside these statutes, however, courts are rather reluctant to hold tortfeasors strictly liable. A particular feature of Swedish law is the existence of alternative no-fault compensation schemes with respect to injuries of patients or workers and harm caused by pharmaceutical products.

4.3.1.3.2 Third party liability for airplanes, GMOs, nuclear installations, medical products (pharmaceuticals) and environmental harm

---

222 Including airplanes, genetically modified organisms, nuclear installations, medical products (pharmaceuticals) and environmental harm as outlined below. Further examples are the strict liability of car drivers and car owners under the Road Traffic Act (Straßenverkehrsgezetz; StVG) and of train operators, operators of energy, gas and liquid pipes under the Liability Act (Haftpflichtgesetz, HPflG).

223 Article 6:178 BW: armed conflict, civil war, revolt, riots, insurgence or mutiny; natural event of an exceptional, unavoidable and irresistible nature; the damage is solely caused by following an order or regulation of the government or intentionally caused by a third party or is the result of a nuisance, pollution or any other consequence for which no liability would have existed on the basis of the general principles of tort law if the defendant had caused it intentionally.

224 Dziennik Ustaw (Journal of Laws, Dz U) 2009, no 62, at 504 as amended.

225 For the explanation of some of these strict liability statutes see below.
Airplanes

In Europe liability of the air carrier for damage caused to passengers is regulated by Reg 889/02,226 which is based on the Warsaw Convention of 12 October 1929227 as amended by the Montreal Convention of 28 May 1999228 (see chapter 5.1.2.). According to the Warsaw-Montreal regime, the air carrier is obliged to compensate passengers for death and bodily injury for up to 113,100 special drawing rights (SDR) subject only to the defence of contributory fault of the victim (Article 20 and 21 Montreal Convention). For damage exceeding this cap the air carrier is liable according to fault based liability with presumption of fault. The air carrier is exonerated if he proves that the damage was not due to the negligence or other wrongful act or omission of the carrier or its servants or agents, or that the damage was solely due to the negligence or other wrongful act or omission of a third party (Article 21 (2) Montreal Convention). With respect to baggage and cargo, special rules and liability caps apply (Article 17 et seq Montreal Convention). Reg 889/02 extends these rules to all flights, whether domestic or international, operated by Community air carriers and provides some rules favourable to the harmed passenger (advance payments in the event of bodily injury, jurisdiction of the courts of the passenger's principal place of residence; increase of liability limits in the event of delay and damage to baggage). Minimum insurance requirements for air carriers and aircraft operators in respect of passengers, baggage, cargo and third parties, for both commercial and private flights are provided by Reg 785/04 on insurance requirements for air carriers and aircraft operators as amended by Reg 1137/08 and 285/10.229 The objective of this Regulation is to establish minimum insurance requirements for air carriers and aircraft operators in respect of passengers, baggage, cargo and third parties to cover the risks associated with aviation-specific liability (including acts of war, terrorism, hijacking, acts of sabotage, unlawful seizure of aircraft and civil commotion).

Damage to persons other than passengers is regulated by the national laws. Of all the countries that are analysed in this comparison only Spain is a party to the 1952 Rome Convention (see chapter 5.1.1).

Most countries provide for special strict liability rules for airplane accidents. In England and Wales, aircraft owners are strictly liable for all material loss to third parties (section 76 (2) of the Civil Aviation Act 1982). Liability is unlimited in amount and only subject to a defence of contributory negligence. In France strict liability is provided by the Code of Transports. German law also provides for comprehensive strict liability for damage caused by airplanes. According to § 33 LuftVG,230 the owner of the airplane is strictly liable for damage to the life, physical integrity or health of a person or to property caused by an accident. This strict liability obligation applies to any third party who uses the airplane without the consent and knowledge of the owner (§ 33 para 2 sent 1 LuftVG). The rules on contributory fault, joint and several liability and heads of damages are in line with the general rules of the BGB (§§ 34 et seq LuftVG). Liability is capped according to the weight of the airplane. In Poland strict

227 Convention for the Unification of Certain Rules Relating to International Carriage by Air (Warsaw, 12 October 1929; 4 UST 5250; 137 LNTS 11; (1963) ATS 18).
liability for the operator of an aircraft is provided by a special statute. As the law refers to liability based on Article 435 of the Polish civil code, the operator is not liable in cases of force majeure, or if he proves that the damage was caused exclusively through the fault of the injured party or of a third party for whom he is not responsible. In Spain third party liability for the operator of an airplane is regulated by the act of aeronautical navigation (LNA). This Act provides for strict liability connected with compulsory insurance and liability caps. According to Article 121 LNA, the airline or operator is additionally liable under fault based liability if the employee acted with intent or gross negligence. In Sweden, the Act on liability for damage caused in the course of aviation from 1922 provides for non-contractual strict liability of the owner of the aircraft regarding personal injuries and property damage on the ground. Dutch law do not provide for special liability rules for the victims of airplane accidents. Third parties who are victims of an airplane accident must thus rely on the general tort law system.

Genetically modified organisms
Of all the countries analysed, only Germany and Poland provide for specific strict liability statutes covering liability for GMOs. French law only provides for public law obligations which however can lead to compensation obligations under civil law.

England and Wales, the Netherlands and Sweden have no special liability rules for genetically modified organisms. In the Netherlands it is still unclear whether the strict liability for dangerous substances (Article 6:175 BW) applies to damage caused by GMOs.

Nuclear installations
In all the countries analysed, third party liability for nuclear installations is determined by the international convention on nuclear third party liability (see chapter 5.2). Germany, France, the Netherlands, Spain, Sweden and the United Kingdom belong to the Paris and Brussels Conventions on Nuclear Third Party Liability. The Paris Convention provides for the elaboration and harmonisation of third party liability and insurance against nuclear risks. The 1963 Brussels Supplementary Convention, which is only open for members of the Paris Convention, supplements the Paris Convention by providing for additional compensation out of public funds. On February 12, 2004 the Member States of the Paris Convention, signed a new Protocol to the Paris Convention and a new Protocol to the 1963 Brussels Supplementary Convention. Both new protocols form an integral part of the relevant convention, but are not yet in force.

---

232 Ley de Navegación Aérea de 21 de junio de 1960.
233 Lagen (1922:382) angående ansvarighet för skada i följd av luftfart.
236 For a comprehensive description and analysis of these regimes and for liability for genetically modified organisms in other countries see Koch 2010.
Poland belongs to the 1963 Vienna Convention\textsuperscript{243} and the 1997 Protocol to the Vienna Convention.\textsuperscript{244} The Paris and the Vienna Convention are linked together by the 1988 Joint Protocol\textsuperscript{245}, which mutually extends the benefits of one convention to the members of the other convention. Four of the countries analysed (Germany, Netherlands, Poland and Sweden) belong to the Joint Protocol, while three countries (France, Spain and the United Kingdom) do not.

All the nuclear liability conventions provide for non-fault liability for damage caused by a nuclear incident. Liability is concentrated on the operator of a nuclear installation (“legal channelling”). Liability of the operator covers nuclear incidents in a nuclear installation or involving nuclear substances coming from such an installation, and also under certain conditions, nuclear incidents occurring during the carriage of nuclear substances. The concept of legal channelling ensures that claims for the compensation of nuclear damage may only be directed against the operator of a nuclear installation and not against any other person, such as suppliers, carriers, contractors or other third parties. Such persons are not liable at all, neither under the specific nuclear liability regime established by the convention nor according to other liability provisions provided by national tort law, such as product liability\textsuperscript{246} or fault based liability.\textsuperscript{247} In order to ensure that the risk is in any case allocated to the operator, Article 6 (f) of the 1960 Paris Convention even limits the operator’s right to recourse. Recourse is only available, if an individual person (but not a legal entity) has intentionally caused the damage, or if the right to recourse is expressly provided by contract. The second goal of legal channelling is to restrict the operator’s liability. This means that the operator’s liability is exclusively regulated by the convention and the national laws implementing it.

The operator is obliged to provide for financial security (principle of congruence of liability and coverage). In order to exclude forum shopping, jurisdiction only lies with the courts of the Member State in whose territory the nuclear incident occurred, or, if the nuclear incident occurs outside the territory of the state, or, if the place of the nuclear incident cannot be determined with certainty, with the courts of the member state in whose territory the nuclear installation of the liable operator is situated (“exclusive jurisdiction”). Applicable law, both substantive and procedural, which is not specifically governed by the convention, is the law of the competent court (\textit{lex fori}). The nature, form and extent of the compensation, as well as distribution matters are regulated by national law. The Paris Convention, and the national laws implementing it, must be applied without any discrimination based upon nationality, domicile, or residence in order to ensure equal treatment of victims (principle of non-discrimination). Judgments that are enforceable under the jurisdiction of the competent court must be recognised and enforced in all the other Member States. Compensation, insurance and reinsurance premiums, including interests and costs, must be freely transferable between the contracting countries.

Liability is limited in amount and time. Article 7 (b) of the 1960 Paris Convention provides that the maximum liability of the operator with regard to damage caused by a nuclear incident

\begin{itemize}
\item[243] Vienna Convention on Civil Liability for Nuclear Damage (Vienna, 21 May 1963; IAEA INFCIRC/500).
\item[247] There are only two exceptions: According to Article 6 (c) (i) of the Paris Convention, the convention does not prevent (1) liability of an individual who intentionally caused damage by a nuclear incident, and (2) liability of a person duly authorised to operate a reactor comprised in a means of transport, if the operator’s liability is excluded by the convention.
\end{itemize}
is 15 million Special Drawing Rights (SDR) of the International Monetary Fund (approximately € 18.2 million). In order to cover this liability, the operator is obliged to have and to maintain insurance or other financial security for this amount. Member States, taking into account the operator’s possibilities of obtaining coverage, are allowed to provide for a lower or higher liability cap by legislation, or – despite the principle of congruence of liability and coverage – even unlimited liability. With regard to less dangerous nuclear installations and substances, the liability cap may also be reduced. The minimum amount of liability and coverage is 5 million SDR (approximately € 6.1 million). The 2004 PC-Protocol increases liability sums substantially. It establishes a minimum amount of € 700 million(Article I (H) 2004 PC-Protocol). This minimum liability cap of € 700 million cannot be reduced according to the capacity of the insurance market, as was provided by Article 7 (b) (i) of the 1960 Paris Convention. Thus, Member States are only allowed to deviate from this amount by establishing a higher liability cap or unlimited liability by national legislation. Signatory states of the 2004 PC-Protocol may establish a lower liability cap of at least € 70 million for less dangerous nuclear installations, and at least € 80 million for the carriage of nuclear substances (Article I (H) 2004 PC-Protocol). Interests and costs are not considered to be compensation for the purposes of the convention. Thus, if they are awarded by a court, they must be paid by the liable operator in addition to the compensation sum (Article I (H) 2004 PC-Protocol).

The operator of a nuclear installation has only very few defences available. According to Article 9 of the 1960 Paris Convention, the operator is not liable for harm caused by a nuclear incident directly due to an act of armed conflict, hostilities, civil war, or insurrection. If the damage is caused by a natural disaster of an exceptional character, the 1960 Paris Convention allows for a defence, unless provided otherwise by national legislation. The 2004 PC-Protocol eliminates this exoneration (Article I (J)). Thus the operator of a nuclear installation will also be liable for damage directly caused by a natural disaster, be it of an exceptional character or not. The 2004 PC-Protocol, however, allows national law to provide for a defence of contributory negligence in case of gross negligence or the intentional actions of the person suffering the damage (Article I (G) 2004 PC-Protocol).

In England and Wales the Paris and Brussels Conventions were implemented by the Nuclear Installations Act 1965 which provides for a liability cap of £140 million per nuclear incident. In April 2012 the UK government announced its intention to implement the 2004 Protocols to the Paris and the Brussels Convention, which will increase the existing operator liability limit of £140 million per incident to €1200 million.

France already increased the operator liability to the level of the 2004 Protocols, which is € 700 million per nuclear incident by Law of 13 June 2006 (which amended Law n° 68-943 of 30 October 1968). This amendment also introduced the defence of gross negligence of the victim. The liability caps for ‘reduced risk installations’ (as defined by decree n° 91-335 of 12 April 1991) and for the transport of nuclear materials, if the transport is covered by the Paris Convention, specifically € 70 million and € 80 million respectively, are also in line with the 2004 Protocols. If the transport is not covered by the Paris Convention, the liability cap is increased to € 1.2 billion. Compensation provided by the State according to the Brussels Convention is € 1.5 billion. In the event that loss for personal injury exceeds this amount, further compensation will be provided by special decree. Special rules apply for the liability for damage caused by nuclear ships, implementing the Brussels Convention of 25 May

---

In Germany, the Nuclear Power Act (Atomgesetz) declared the Paris Convention directly applicable. It, however, provides for several deviations from the convention, most importantly for unlimited liability of the operator. Limitations only apply with respect to damage in another country with limitations (reciprocity) and in exceptional cases such as natural disasters or war where there is a cap of € 2.5 billion Euro.

In the Netherlands, the Paris-Brussels regime is implemented by the Nuclear Accidents Liability Act (‘Wet aansprakelijkheid kernongevallen’), which provides from 1 January 2013 onwards a cap of € 1.2 billion. In Spain, the liability cap is € 700 as provided by the Act on civil liability for nuclear damage of 28 May 2011, and in Sweden, where the actual liability cap is set at 300 million SDR, the new act on nuclear liability which is not yet in force will provide for unlimited liability with the obligation for coverage by insurance for up to 1.2 billion Euro.

In Poland, where the obligations derived from the Vienna Convention were implemented by Title 12 (Articles 100 – 108) of the Polish Atomic Law, the liability cap is set at 300 million SDR. If claims exceed the limit, a special fund must be created. In addition, the State covers the compensation for damage to persons above the sum guaranteed in the insurance policy.

Medical products (pharmaceuticals)

The only country which provides for a special strict liability regime for medical products is Germany. According to the German Pharmaceuticals Act (Arzneimittelgesetz; AMG) the producer of a medical product that is intended for human use is strictly liable for damage caused by the product. The development risk defence does not apply. Liability is capped and there is obligatory financial coverage. Claims on the basis of fault based liability and product liability remain unaffected (§ 91 AMG).

In France professionals in the health sector are under an obligation to secure the security of health products they use (see Law no 2002-203 of 4 March 2002). The Netherlands, Poland and Spain do not provide for specific liability rules for medical products. In all of these countries the liability for pharmaceuticals is regulated by product liability law with the peculiarity that in France the development risk does not apply for medicinal products derived from the human body and in Spain to medicines in general. In Sweden injuries caused by pharmaceuticals are covered by a no-fault insurance scheme set up by the pharmaceutical industry.

Environmental harm

Dir 35/04 on environmental liability with regard to the prevention and remedying of environmental damage which harmonised the rules on the prevention and restoration of site damage.
contamination and on loss of biodiversity in the European Union (see chapter 3.1.) has not interfered with national tort law remedies for the compensation of environmental harm. The picture of liability for environmental harm is thus very heterogenous in the countries analysed. Environmental damage underlies the rules of general tort law including nuisance law and general strict liability regimes, such as Article 1384 (1) of the French Code civil (liability of the custodian of a thing) or Article 435 of the Polish civil code which, according to Article 324 Environmental Protection Law of 27 April 2001,\(^{258}\) does not require that the installation is run with the use of natural forces if the installation is dangerous. In Spain, environmental harm is covered by Article 1908 Código Civil which provides for strict liability for harm to persons and property caused by toxic fumes.

Specific and comprehensive strict liability regimes for environmental harm are provided in Germany and Sweden. The German Environmental Liability Act 1990 (UmwHG) imposes strict liability on the operator of certain dangerous installations exhaustively listed in Annex 1 to the UmwHG. An exclusion applies in the case of force majeure (§ 4 UmwHG). \(^{259}\) § 6 UmwHG provides for a rebuttable presumption of causation. Liability is limited in amount to a maximum of € 85 million per environmental impact incident and liability for negligible property damage is excluded. The act does not cover damage to the environment if it does not constitute property damage or personal injury. A special strict liability rule is provided for damage to water, including the ground water (§ 89 (2) Water Management Law). \(^{259}\) In Sweden, chapter 32 of the Environmental Code provides for strict liability for the owner, or the keeper of land, concerning personal injury, property damage and substantial pure economic loss. With respect to this cause of liability, the burden for the proof of causality is reduced from high probability as required by general tort law to the balance of probabilities. Compulsory environmental clean-up insurance for hazardous activities, originally provided in the Environmental Code, was abolished in 2010. English law has no comprehensive regime of liability in respect of environmental harm. A special cause of action for harm caused by controlled waste is provided by the Environmental Protection Act 1990. \(^{260}\) French law provides for a special insurance compensation mechanism in case of damage which is declared a technological disaster by the administrative authority. \(^{261}\)

4.3.2. Relationship between tort liability and regulation

4.3.2.1. Relationship between tort liability and regulation in general

The relationship of tort liability with regulation is rather complex. Compliance with regulation does not affect strict liability obligations or, as a general rule which has its exceptions, liability according to neighbourhood liability (nuisance). It has, however, important relevance for the application of fault based liability in civil law systems and the tort of negligence in common law.

In all the jurisdictions, public law standards are used by courts to determine the required standard of care. \(^{262}\) They can also be an important source for establishing a legal duty to act in

\(^{258}\) Dz U 2001, no 62, at 627 as amended.
\(^{259}\) Wasserhaushaltsgesetz, BGBl 2009 I, 2585.
\(^{260}\) Section 73 (6) of the Environmental Protection Act 1990: liability for the breach of statutory duty of section 34 (1) Environmental Protection Act 1990.
\(^{262}\) This, as the German reporter points out, also applies to technical standards provided by national or international Standardisation Committees, such as the International Standardisation Organisation (ISO) or the European Committee for Standardisation (CEN) or, as the French reporter indicates, even to internal company regulations or professional codes of ethics.
order to prevent the occurrence of damage. Courts, however, use these standards only as an
indication of what the required standard in general is and do not feel bound by it for the
individual case. It is a general rule that compliance with public law standards does not exempt
the defendant from tort liability. All of the reporters stress that courts will assess the
required duty of care according to the individual circumstances of the case. Private law
standards thus can surpass the standards set by public law. An exception only applies in those
special circumstances when the harm is caused because of compliance with mandatory
regulations issued by the public authorities, as is for instance provided by Article 7 (d)
Product Liability Directive or Article 8 (3) (b) Environmental Liability Directive.

Failure to comply with regulation, however, is in all jurisdictions a strong indication that the
defendant breached the required standard of care (common law) or acted unlawfully or with
fault (civil law). Statutory rules may also serve as rules with a protective scope
(Schutzgesetz). Whether this is the case, is a matter of construction. According to the theory
of the protective scope of the rule (Schutzzwecklehre), which is accepted in many civil law
jurisdictions (see the German, Dutch, Swedish and Spanish reports), the breach of certain
regulatory duties which aim to protect the concrete victim affects tort liability in a twofold
way. On the one hand, it establishes unlawfulness and on the other hand it concretises
the scope of liability with respect to the group of persons protected by the rule and the type of
compensable damages. In English law the breach of a statutory duty constitutes a distinctive
tort in its own right and allows the award of damages to the person injured by the breach if he
belongs to the group protected by the statute.

4.3.2.2. Specific regulations governing the risks of the security industry

Some activities of security enterprises are covered by more general legislation concerning the
use of security devices, like weapons or monitoring devices, or rules regarding the safety of
software.

Several countries (France, the Netherlands, Poland and Sweden) provide for special rules
concerning the licensing of security enterprises and the supervision of their activities which
establish quality requirements and rules concerning the competence and training of the
employees. These rules are enforced by public agencies. Special rules apply with respect to
airport security.

4.3.3. Causation

4.3.3.1. Standard burden of proof regarding the burden of proof of causation

In principle, the burden of proof for causation falls on the claimant. In English and Dutch law
the required standard of proof for the proof of causation is the balance of probabilities. In
Sweden the required standard is very high (certainty beyond reasonable doubt), but in
complex cases of causation courts are inclined to apply a somewhat lower burden of proof
(‘clearly more probable’ than any other explanation). The Spanish reporter did not relate to
any degree of probability but rather stressed that the Spanish courts require that the facts are
established to the conviction of the court. In medical liability and other fields of technological
complexity reasonable probability may already suffice to prove causation in Spanish law. The

263 See the answers to Case 1, question f.
264 Regulation (EC) 300/08 of the European Parliament and of the Council on common rules in the field of civil
same seems to apply in France where the courts, however, are more easily inclined to assume causation in complex cases where causation is difficult to establish. In Germany the standard is a very high level of probability. This is nowadays also the level required by the Polish courts which used to require a very high level of probability close to certainty (beyond reasonable doubt). In Poland this relaxation is mainly applied in complex causation scenarios involving personal injury, but not for claims for lost profits. With respect to public authority liability, liability for animals and personal liability of minors or incompetent persons, the level is even lowered to the balance of probabilities which, according to scholarly opinions, should also be the standard in cases of nuclear liability.

4.3.3.2. Instruments to lighten the burden of proof regarding the proof of causation

Causation is usually established with the so-called ‘but for-test’ according to which causation is not established unless it is shown that the damage would not have occurred without the factor in question. In England and Wales, the connection must be proved according to the balance of probability standard. In France the theories of ‘direct link’ or ‘adequate causation’ are sometimes invoked as well.

In all the countries analysed, courts have some discretion with respect to the establishment of causation. In complex situations, especially in medical liability cases, or in cases involving multiple causes, various strategies are applied to lighten the burden of proof for the claimant. These strategies are rather diverse and range from the classical prima facie evidence (Germany) or res ipsa loquitur (England and Wales, Netherlands, Poland) to more sophisticated strategies in order to cope with only statistical evidence like the attribution of damages according to the loss of a chance (France, Netherlands), or proportional liability (Netherlands), or the English ‘doubles the risk’ test, where the claimant can establish causation by showing that the defendant’s breach doubled the original statistical risk. Some jurisdictions also provide for presumptions of causation. In the Netherlands courts may reverse the burden of proof if this is seen as reasonable and fair (Article 150 Code of Civil Procedure). In France presumptions of causation are applied with respect to certain diseases (HIV, hepatitis C, DES-litigation) and in Poland in pollution cases.

4.3.4. Attribution of liability

4.3.4.1. Multiple parties

If the separate and independent acts of two or several tortfeasors cause separate injuries or divisible harm, the liability of each defendant is limited to the extent of his contribution to the overall harm. All jurisdictions provide for joint and several liability if two or more tortfeasors cause harm to the victim as part of a joint venture. The same applies if the tortfeasors act independently and separately and the harm is indivisible. As a consequence each tortfeasor can be sued by the victim for the entire sum of compensation. In the civil law systems this is explicitly provided in most of the civil codes. In France it was established by case law and in Spain this rule is explicitly provided only in special liability statutes and the criminal code but generally recognised by case law and scholarship.

The tortfeasor who compensated the victim then has a right of recourse against the other contributors. The decisive criteria for the assessment of the shares of the contributors differ in the various countries. In Germany the general rule of the BGB (§ 426 BGB) is apportionment per capita, while in products and pharmaceutical liability apportionment is conducted according to the particular circumstances of the individual case. In the Netherlands the apportionment is the result of a more comprehensive assessment which includes fault, the individual circumstances of the case and equity. English and Polish law also refer to the
circumstances of the case, in particular to the fault of each contributor and the degree to which the latter contributed to the occurrence of the damage. In Swedish law, the damages must be apportioned according to what is reasonable, but in fact, as the Swedish reporters indicate, the main factor is the seriousness of fault of each contributor.

If the liability was incurred without fault, it is split in equal shares in most countries. In some jurisdictions (England and Wales, Poland and Sweden) it is held that in case of concurrence of fault based liability and strict liability, the contributor who was at fault has to bear the whole damage.

4.3.4.2. Legal channelling of liability to one person

Legal channelling, as provided in nuclear liability law according to the nuclear liability conventions and the national implementation laws, is not a general feature of the national tort laws. If damage is caused by multiple parties, the harmed person can claim damages from each tortfeasor according to the cause of action applicable to this tortfeasor, and the tortfeasor who indemnified the claimant will have a right of recourse against the others. Channelling of liability against the operator of an activity, as is provided by strict liability statutes, does not amount to legal channelling in this sense as liability of persons other than the operator will not be excluded.

Instruments that come close to legal channelling are the rare exceptions. A certain degree of channelling is achieved by vicarious liability. No national law, however, totally excludes liability of the employee towards the third party and the right of recourse of the employer. Another example can be found in Sweden for recourse of insurances with respect to property damage caused by someone’s employee (vicarious liability) or by the state or municipality. Legislative plans to channel liability for terrorist attacks to the state which were discussed in Sweden for some time have so far been rejected.

4.3.5. Damages and available remedies

4.3.5.1. Types of compensable damages

It is generally accepted in all of the jurisdictions that tort liability covers personal injury, property damage and consequential financial loss. This includes damages for pain and suffering. This applies now also to German law which did not provide for damages for pain and suffering in strict liability statutes in the past, but eliminated this restriction in 2002. Compensation for other types of non-pecuniary loss is often restricted to certain specific cases (eg Germany, Netherlands, Poland).

The compensability of pure economic loss is more disputed. In England and Wales pure economic loss is only recoverable under exceptional circumstances. The same applies in Germany, where pure economic loss is not covered by the general tort law provision of § 823 (1) BGB, but only by § 826 BGB for the intentional infliction of damage in a manner contrary to public policy and by § 823 (2) BGB on breach of a statutory duty. That statutory duty, however, must have the purpose of protecting the victim’s patrimony independently from physical injury or damage to property. In Sweden, pure economic loss is only compensable if the loss was caused by a criminal act (Chapter 2 section 2 Tort Liability Act) and, according

265 BGBl 2002 I, 2634.
to case law, if there is a relationship of reliance between the tortfeasor and the claimant. Moreover, some strict tort liability statutes offer special protection for pure economic loss.

French, Dutch, Polish and Spanish law follow the principle of full compensation and do not distinguish pure economic loss as a separate head of damage in general tort law. Compensation includes non-pecuniary and pure economic loss. The most comprehensive view is taken by French law which follows the principle of full compensation including non-pecuniary and pure economic loss. In the past, French courts did not to specify the heads of damages when they attributed compensation. This has changed with respect to personal injury where the ‘nomenclature Dintilhac’ is now widely used which distinguishes between temporary and permanent harm and pecuniary and non-pecuniary loss. These countries restrict the compensability of pure economic loss, however, through considerations of causality and attribution of the loss. French and Spanish law require a sufficiently direct causal link between the tortious behaviour and the damage. For liability for breach of contract, Article 1150 of the French civil code requires that the loss was foreseeable when the contract was concluded. In Poland such a limiting effect is brought about by the concept of adequate causation established by Article 361 § 1 of the Polish civil code. This limit is excluded when the breach was particularly serious, which is the case when the tortfeasor acted with intent or with gross negligence. In the Netherlands Article 6:98 BW provides that damage shall be attributed according to the nature of the damage and the nature of the liability. Foreseeability, although not expressly mentioned, also plays an important role. Courts thus have a considerable margin of discretion in the attribution of damage to the tortfeasor, which is exercised differently for the different types of damage.

In English and German tort law, environmental harm is not a recognised head of damage. It is only compensable if it constitutes property damage or personal injury. But like in the Netherlands, as described by the Dutch reporter, the costs for clean-up and prevention of environmental damage are recoverable as pecuniary loss under general tort law provided that the claimant can show a sufficient legal interest in the measure. This is at any rate the case with the owner of the polluted property. The Netherlands go one step further and grant legal standing also to associations or foundations with vested interests in environmental matters. The same principles apply in Poland, but, in addition, Polish law allows certain institutions (State Treasury, local authorities or ecological organisations) to sue for compensation for harm to the environment under the Environmental Protection Law (Articles 322 et seq) and the Law on GMOs (Article 57 subsec 2). In Sweden, the Environmental Code provides for strict liability for personal injuries, property damage and pure economic loss caused by emissions or disturbances from an activity on a nearby property including environmental clean-up. The most comprehensive recognition of environmental damage is provided by French law, where it has become a special head of damage in tort law. Environmental damage is addressed in several environmental regulations and was recently recognised as head of damage by the French Supreme Court (Cour de cassation). It covers property damage, pure economic loss, remedial action including the cost of remedial action and even non-pecuniary damage. In case of pure ecological damage (e.g. loss of biodiversity) special interest groups (nature protection associations) may be entitled to claim damages. It is even intended to implement the concept of ‘environmental damage’ into the French civil code.

---

266 Chapter 32 of the Environmental Code and Section 7 (3) of the new Nuclear Liability Act.
267 See French report, Case 1 question e and Case 2 questions a, d; Spanish report, Case 2 question d.
268 See French report, Case 2 question a.
269 For liability under Dir 35/04 on environmental liability with regard to the prevention and remedying of environmental damage see section 4.3.1.3.2 above.
4.3.5.2. Exclusion of heads of damage by contractual agreement

In all the analysed countries except in France tort law liability can be limited by contractual stipulation. This contractual freedom is, however, limited by various rules concerning special heads of liability which prohibit the contractual limitation or exclusion of liability as is for instance provided by Article 12 of the Product Liability Directive. For general tort law, due to **Dir 13/93 on unfair terms in consumer contracts**, it is common standard in all the countries that in B to C (business to consumer) relationships, fault based liability for personal injury cannot be excluded or limited by standard terms. In most countries this rule is extended to B to B (business to business) relationships, as such terms do not pass the required reasonableness-test (eg Germany, Netherlands, Poland). In the same context, English law does not distinguish between consumer and business contracts and, according to Article 2 of the Unfair Contract Terms Act 1977, declares contractual clauses that exclude liability for death or personal injury resulting from negligence void. Clauses excluding liability for any other loss or damage resulting from negligence are subject to a test of reasonableness and are void, if unreasonable. As regards exclusion clauses in relation to liability for breach of contract, a test of reasonableness will also apply if one of the parties is dealing as a consumer or if the contract is conducted using written standard terms of business.

In Germany any exclusion or limitation of liability for damage to property arising from a grossly negligent breach of duty is ineffective. In the Netherlands and in Spain such clauses are subject to a test of reasonableness. Although exclusion or contractual limitation of liability is in principle allowed in contracts in B to B (business to business) relationships, such exclusions can be tested under general fairness rules including the assessment of such factors as the relative bargaining powers, the degree of fault and the extent and nature of the losses incurred.

4.3.5.3. Special instruments for mitigating the liability of the tortfeasor (liability caps, reduction clauses)

No country provides for a **liability cap** for fault based liability. In Germany and Spain liability caps are quite usual in strict liability statutes. In the Netherlands liability caps can be provided by the executive according to Article 6:110 BW, but so far no limitations have been introduced. For particular providers of services (pilots, air traffic controllers) and certain public authorities (Bank of Netherlands, Financial Markets Authority) liability is restricted to intentional, grossly negligent or willfully reckless behaviour. In France and Poland liability caps are mainly provided in fields of liability that are regulated by international conventions (eg nuclear liability) and for hotel keepers (Article 849 § 1 Polish civil code; Article 1953 al. 3 and Article 1954 al. 2 French Code civil). In France liability caps are also provided for transportation and by certain compensation schemes (workers compensation, natural disasters etc). In Sweden the special alternative compensation schemes for patients or pharmaceuticals are subject to caps. In tort liability Swedish law does not accept liability caps and will in future even provide for unlimited liability in nuclear liability law.

**Reduction clauses** are not a common instrument for mitigating the liability of the tortfeasor. Of all the analysed countries only the Netherlands (Article 6:109 BW) and Poland (Article 440 CC) have such explicit rules, but in both countries this instrument has not yet been widely used. According to Article 440 of the Polish civil code, the reduction clause can be applied only to physical persons. It allows only the reduction and not the total exclusion of damages

---

and is not applied in cases of intentional fault, gross negligence or personal injury or where the person liable has liability insurance cover. In Spain, Article 1103 CC allows courts to mitigate damage arising from negligence on a case-by-case basis. Compensation for personal injuries and death is often awarded according to a tariff system developed for road traffic accidents that is now under revision.

4.3.6. Applicability in time (retrospective liability)

The introduction of retrospective liability by the legislature is seen as a rather problematic measure by all the reporters. Of all the reporters only the reporter for England and Wales considers this measure to be admissible although “generally frowned upon”. All the other reporters are of the opinion that such a measure is not accepted by law (Germany, Sweden), or would at least be very unusual (France, Netherlands), or are not literally impossible, but must be explicitly provided by the respective legal provision (Poland, Spain).

4.3.7. Alternative compensation mechanisms

4.3.7.1. Alternative compensation schemes

The picture concerning alternative compensation mechanisms is very heterogeneous. All the countries provide for compulsory liability insurance in certain areas (motor vehicles, airplanes, nuclear installations etc). In Poland, security companies which provide for security services directed at the guarding of human life and property at airports are obliged to take out liability insurance.\(^{273}\) According to the regulation issued by the Ministry of Finance on 4 October 2012,\(^{274}\) the insurance does not cover inter alia war risks, hostilities and acts of terror. All damages are covered and the insurer may not limit its liability. The minimum guarantee sum for the period of coverage of maximum 12 months is set at 5,000 SDR per 1,000 passengers serviced or 5,000 SDR per 100,000 kg of cargo or post serviced in the previous year, whichever sum is higher. If the company carries out its services on more than one airport, the minimum guarantee sum must be the higher sum that applies to a given airport.

All countries have special rules concerning the coverage of personal injury by social security which are, however, very different, and all countries have compensation funds for specific areas, eg for crime victims (Germany, France, Spain, Sweden and UK),\(^{275}\) natural disasters (France), technological disasters (France), patient and pharmaceutical injuries (Sweden), or vaccine damage (UK) and workers’ injuries (Sweden).

4.3.7.2. Compensation schemes for victims of terrorism

Special compensation schemes for victims of terrorism are provided in France, Spain and the UK.\(^{276}\) The British compensation scheme was introduced in 2012, and covers victims of overseas and domestic terrorism\(^{277}\) who cannot obtain compensation from other sources.

---


\(^{274}\) Dz U 2012, item 1123.

\(^{275}\) Koch, 2010, CS 11 (p 263).

\(^{276}\) For an explanation of the new terrorism insurance schemes see chapter 6.3.5.

Payments are calculated by reference to a tariff system similar to the one used for the Criminal Injuries Compensation Scheme, with a maximum individual payment of £ 500,000.

In France the Law of 9 September 1986 created a compensation fund for the victims of acts of terrorism (FGTI) which is funded by a tax on property insurance contracts. This fund compensates only personal injuries. For property damage, compensation must be provided by the insurers. Following the attacks of 11 September 2001, insurers refused to continue to cover some of these risks, and they are now shared between insurers, reinsurers and the state.

In Spain, the 2011 Act of Recognition and Comprehensive Protection of Victims of Terrorism provides subsidies to victims in case of death, personal injury and kidnapping caused by terrorists. It also provides contributions for damage caused to cars, industrial or commercial establishments and to the headquarters of political parties and trade unions. The French and the Spanish act provide for subrogation.

4.3.7.3. Special rules on case management

All of the national legal systems analysed provide for special rules on case management. The approaches towards collective redress, however, vary a lot. Traditional mechanisms of joining of actions, like joinder of parties can be observed in all national legal systems. The legal solutions concerning further collective redress mechanisms are rather unique and can thus hardly be compared. In the last few years a trend towards the introduction of new collective redress mechanisms can be observed in various Member States. New mechanisms have been created recently in Germany (a group action for capital market law claims and a skimming-off procedure for unfair competition law cases), in the Netherlands (a collective settlement procedure) and in Poland (group action for claims of consumer protection, claims based on product liability and claims based on tort law). Group actions are also available in the UK, in Spain and in Sweden. Nevertheless none of the national legal systems analysed provides for a US-style class action.

4.3.8. Suggested reforms in national literature

In some countries reforms of tort liability in general (France) or with respect to special issues (Germany: introduction of collective redress mechanism or of market share liability; Poland: expansion of strict liability to dangerous activities in general) are under discussion. There are, however, no reform plans or discussions regarding the liability of the security industry in any of the jurisdictions analysed. In Sweden the issue of liability of the airport operator in case of terrorism has been discussed, in concreto with respect to channelling the liability to the state, but the legislative intervention has been rejected.

---

279 Ley 29/2011, de 22 septiembre de Reconocimiento y Protección Integral a las Víctimas del Terrorismo.
280 Annex I of the LRPIVT contain the following amounts for different kinds of injuries with permanent effect. Death € 250,000.00; severe disability € 500,000.00; absolute permanent disability € 180,000.00; total permanent disability € 100,000.00; partial permanent disability € 75,000.00.
281 Capital Market Model Claims Act (Kapitalanleger-Musterverfahrensgesetz [KapMuG]) and § 10 of the Unfair Competition Act (UWG).
282 Dutch Collective Settlement of Mass Damage Act (Wet Collectieve Afwikkeling Massaschade [WCAM]).
283 The Act of 17 December 2009 on Pursuing Claims in Group Proceedings, Dz U 2010, no 7, item 44.
4.3.9. Successes and failures of the national approach

The jurisdictions analysed do not provide for specific tort law solutions for the liability risk of the security industry. It is common opinion among the national reporters that there is no specific need for such provisions. According to the English reporter the existing general tort law achieves an ‘acceptable balance between the interests of claimants and defendants’ and the Dutch reporters outright deny the need of special treatment for the security industry. The Swedish reporters indicate the heterogeneity of the risk posed by the security industry and doubt whether these different types of risks would qualify for any special intervention from the legislator or the creation of any compensation scheme that can fit into Swedish law. They stress the importance of methods of soft law regulation for the liability risk of the security industry, as provided by the insurance agreement between a security company and the insurer or the security service contract between the security company and the client.

4.4. The liability risks of the security industry

4.4.1. The liability risk of the security company towards the client

Towards the client the security company is liable according to the contract concluded between the company and the client. The liability covers damages sustained by the client because of the fault of the security company including fault of employees by way of vicarious liability and comprises compensation for personal injury, property damage and pure economic loss.

The particulars of the liability of the security company are determined by the concrete contract. The parties are relatively free to shape the contents of the contract including stipulations for the contractual limitation of liability. They may thus limit the contractual liability of the security provider towards the client as well as the mutual recourse obligations of both parties.

The contractual freedom is rather broad and is only limited by national rules concerning the fairness of contractual clauses. According to these rules (see 4.3.5.2.), it would be rather problematic to limit fault based liability for personal injury of the client (which can only play a role if he is a natural person) and his employees and to restrict the compensation of damage to property caused by gross negligence of the security provider. These restrictions, however, only apply for the direct liability of the security provider for such harm (damage to person and property) sustained by the client and his employees. They do not apply to other heads of damage (pure economic loss, environmental damage) and to the recourse obligation of the security provider for damage of third parties that were compensated by the client. Moreover, it must be considered that damage sustained by the client’s employees will in many countries be compensated by workmen’s compensation schemes.

4.4.2. The liability risk of the security company towards third parties

4.4.2.1. Direct claims of third parties against the security company

The liability of the security company towards third parties is regulated by the rules of extra-contractual liability. There are two heads of liability available: fault-based liability and product liability, if the harm was caused by a product in the sense of the EU-product liability directive which was put into circulation by the security company.

Fault based liability
All of the jurisdictions analysed provide for a sort of fault based liability. In the common law jurisdiction of England and Wales the most important head of liability is the tort of
negligence, the tort most similar to the concept of fault based liability in civil law (see 4.3.1.1.). Fault based liability in the civil law and negligence in the common law both require the breach of a standard of care.

It is evident that the security provider can only be liable, to the client as well as to third parties, if he enters into a contractual obligation with the client. It is the contract which describes the tasks of the security company and the machinery the security company must use and defines the security measures the company must provide. A company contracted to guard the premises of an industrial facility may, for instance, expressly stipulate that the security measures provided shall only prevent industrial espionage or shall only protect the client’s personnel from personal injury. It must also be possible for the security provider to clarify that the stipulated security measures are not aimed at the prevention of damage caused by an act of sabotage or a terrorist attack. As a specialist, the security provider must meet a high standard according to the special knowledge and abilities of a professional. He must inform the client of the available measures, devices and methods and must warn the client if he realises at the conclusion of the contract or later when fulfilling the contract that the stipulated security measures, devices or methods are inadequate or not sufficient for the stipulated task. If the contract clearly specifies the type of measure, device or method that must be provided by the security provider, then the client cannot claim that the security provider should have taken another measure or should have used another device or method when harm occurs. Liability of the security provider can then only be established for the failure to adequately inform and warn the client.

The wording and contents of the contract not only shape the potential liability towards the client, but also towards third parties. The contract is key in respect of the question of which persons the security provider owes a duty of care, whether only to the client and his employees or also to other persons who permanently or temporarily sojourn on the guarded premises, such as tenants, visitors or shoppers, or even to third parties outside the controlled premises. If harm occurs, the victim who is part of this group is allowed in many countries to sue the security provider directly for damages. The relevant theories in this respect vary. It may be that courts allow the victim to rely on the contract between client and security provider to which is attributed a protective scope for the concrete victim (Vertrag mit Schutzwirkung zu Gunsten Dritter) or courts may conclude that the security provider assumed such responsibility for the concrete victim when he concluded the contract. As the duties of the security provider are specified by the contract, a third party will – like the client – not be able to base a liability claim on the fact that the security provider did not provide a certain service if the security provider is not contractually obliged to render this service (eg to provide video surveillance or to monitor incoming vehicles for explosives). In this case, the security provider will only be liable for the failure to adequately warn the client of the risk so that the client was therefore not able to take adequate measures to prevent the damage. As long as the security provider acts as an auxiliary of the client it is the client who is primarily responsible that third parties are not harmed by his activity. A broad liability for third parties, however, will apply if the security provider contractually takes over the responsibility from the client to provide for the security of a facility or a certain activity. In many countries this situation is described by the theory of the liability of the independent contractor.

In this regard it is important to note that the breach of a contractual duty towards the client does not automatically amount to tortious behaviour towards a third party. Most reporters indicated this quite clearly when they discussed Case 2 of the questionnaire. The reporter for England and Wales explained that English law recognises, according to the ‘Caparo test’, only a duty of care towards the plaintiff if the damage was foreseeable and the requirements of proximity and, as a broad policy consideration, the requirements of fairness, justice and reasonableness are met. In most civil law countries a comparable effect is generated by the criterion of unlawfulness. Only French law allows the third party to rely for the action in tort on the breach of the contractual duty between the security provider and the client, but French
law requires a sufficiently direct link between the incurred damage and the behaviour of the tortfeasor and thus restricts the right to claim damages with reference to considerations of causality. These restrictions apply to all types of damage, but are quite essential for the compensability of pure economic loss sustained by third parties.

In all jurisdictions fault based liability covers damages for personal injury, harm to property and consequential economic loss. Compensation for pure economic loss (see 4.3.5.1) is rather restricted and the rules for the compensation for environmental damage are rather complex and diverse in the various jurisdictions (see under 4.3.5.2.). In England and Wales, Germany and Sweden pure economic loss is only recoverable under exceptional circumstances. In the other countries (France, Netherlands, Poland and Spain), which do not distinguish between pure economic loss and the other heads of damages in the first place, the compensability of pure economic loss is restricted by further considerations, such as the necessity for a sufficiently direct causal link (France, Spain) or by the concept of adequacy (Poland) or by more general considerations (Netherlands).

From the national reporter’s answers to Case 2 (defective safety programmable logic controller) it can be concluded that mistakes by the security provider in the exercise of the contractual duties towards the operator of the undertaking do not necessarily lead to liability for pure economic loss of third parties and for the prevention and remediation of environmental harm.

In the answer to Case 2 the English reporter denied any liability of the security company and the operator of the chemical plant for the cost of the relief measures of the fire brigade (C) and the water supplier (D) or for the lost profits of factory G. Liability of the security provider (under negligence) and of the operator of the chemical plant (under the rule in Rylands v. Fletcher) do not cover pure economic loss or environmental damage. Liability, thus, exists only with respect to the neighbour E, who suffers property damage and personal injury. The French reporter came to the conclusion that the security provider would in any case only be liable for a small share of the losses. Direct liability of the security provider under general fault based liability to third parties seemed rather doubtful to the French reporter, who discussed the responsibility of the security provider primarily under the aspect of contractual recourse of the operator of the chemical plant against the security provider. The recourse action requires under Article 1150 of the French Code civil foreseeability of the damage at the conclusion of the contract and, according to Article 1151 Code civil, a sufficiently direct link between the breach of the contractual duty and the loss. For the concrete case the French reporter doubted the existence of such sufficiently direct link. The German reporter came to a similar conclusion as the English reporter. The security provider and the operator of the chemical plant are only liable to neighbour E who suffered property damage and personal injury. There is no liability of the security provider for the relief measures of the fire brigade C, the water supplier D and the loss sustained by company G, as the security provider is only liable according to fault based liability under § 823 BGB which does not include compensation for pure economic loss and environmental damage. As fault based liability only covers foreseeable damage, the German reporter is of the opinion that the security provider is not liable even if the computer program was especially designed for the prevention of pollution damage in case of natural disasters, if the earthquake was of an exceptional character (Case 2 question b). The operator of the chemical plant is also only liable to neighbour E. Available heads of liability are the strict liability rules in § 1 UmwHG (environmental liability statute) and § 89 (2) Wasserhaushaltsgesetz (Water Act; WHG). Both strict liability statutes (UmwHG, § 89 WHG) provide for an exemption in case of force majeure. The German reporter further discusses the question of whether defective software can be regarded as a product under the product liability directive, which is unclear. This question was also raised by the Dutch and the Spanish reporter.
In Dutch law, like in all the other countries, the security provider is only liable according to fault based liability. The operator of the chemical plant would be liable under Article 6:175 BW which provides for strict liability of the operator of dangerous substances. Both heads of liability would cover the claims of the fire brigade C (given that it was not a public but a private entity), the water supplier D and neighbour E, but both subject to the restriction of Article 6:98 BW which gives courts considerable flexibility for the attribution of the different heads of damage to the tortfeasor. As it is thus in the discretion of the courts whether they award compensation of pure economic loss or not, the Dutch reporter seriously doubts whether the lost profits of company G will be compensable at all. The strict liability of the operator, moreover, underlies a series of defences according to Article 6:178 BW which includes, inter alia, damage resulting from armed conflict, civil war, revolt, riots, insurgence or mutiny, or damage caused by a natural event of an exceptional, unavoidable and irresistible nature, or by an intentional act of a third party. In Spain the operator of the chemical plant B is liable according to the Spanish implementation law of the EU-environmental liability directive for costs of relief measures incurred by the fire brigade C and could claim for contractual recourse from the security provider A. This head of liability does not include the damage sustained by the water supplier D. The neighbour E and the company G could claim damages under general tort law (Articles 1902, 1908 Código civil) which provides for aggravated liability in cases of environmental damage. The company G will only be able to claim the lost profits if the loss is certain and if there is a sufficiently close causal link. The security provider A would be directly liable to the water supplier D and the neighbour E under fault based liability. According to the estimation of the Spanish reporter, no liability will apply to the operator and the security provider if the earth-quake could be seen as an act of god and in case of a terrorist attack. In Sweden the fire brigade C and the water supplier D cannot sue the operator B or the security provider A for the losses sustained, as public authorities are not entitled to claim such damages under general tort law. The operator B is only liable to neighbour E and company G under the strict liability regime of the Environmental Code (chapter 32 section 3), although, according to the estimation of the Swedish reporters, liability towards G may be rejected because of lack of adequate causation. The exceptional strength of the earthquake does not serve as a defence in Swedish tort law which does not provide for such defences outside the implementation acts of international liability conventions, such as the Paris Convention on nuclear liability. Chapter 10 section 19 of the Environmental Code, however, excludes the state’s right to environmental clean-up costs in cases of exceptional natural disasters. With respect to acts of terror, liability under the Environmental Code may be declined pursuant to the notion that strict liability only covers the typical risk of the concrete strict liability regime. An act of terror, however, does not constitute a typical risk for an environmental liability statute. According to the Swedish reporters, the security provider A is not liable at all, as A infringed only a contractual duty towards the operator B and has no non-contractual duty towards third parties like the neighbour E.

The only reporter who held the operator of the chemical plant B and, by way of recourse, also the security provider A to be fully liable was the Polish reporter. The operator of the chemical plant would be liable under strict liability (Article 435 civil code; Environmental Protection Law) and, according to the estimation of the Polish reporter, the operator would in the concrete case not be able to invoke the defence of force majeure, either in the case of the exceptionally strong earthquake or the terrorist attack.

Product liability
If the damage is caused by a product that was put into circulation by the security company, liability is regulated according to the Product Liability Directive. Many reporters stress that

---

287 Dutch report A.I.3.
national courts still apply specific national product liability rules derived from fault based liability (England and Wales, France, Germany, Netherlands).

Liability under the national laws implementing the product liability directive is irrespective of fault. It does not include the compensation of pure economic loss and environmental damage if the environmental damage does not constitute personal injury or property damage. The national laws implementing the Directive follow the rules of the directive very closely, although some deviations gave rise to infringement proceedings before the European Court of Justice. All the countries analysed allow for the development risk defence as provided by Article 7 (e) of the Directive, except for certain products (France: products derived from the human body; Germany: pharmaceuticals; Spain: medicines, food or foodstuffs for human consumption) and, except for Spain, include the recovery of non-pecuniary damages. Germany and Spain provide for liability caps in the case of death or personal injury (Germany: € 85 million; Spain: € 63,106,270.96).

4.4.2.2. Recourse of the client against the security company and vice versa

Heads of liability applicable to the client

Operators of dangerous activities are liable to third parties under fault based liability (common law: negligence), but very often clients of security companies are also subject to strict liability obligations. These are general liability rules with increased liability standards (see 4.3.1.3.1), such as the rule in Rylands v Fletcher in English law, the liability of the custodian of a thing according to Article 1384 (1) French Civil Code ('responsabilité du fait des choses'), liability for the professional use or possession of dangerous substances according to Articles 6:175 Dutch BW et seq, or liability for dangerous undertakings under Article 435 of the Polish civil code. Germany and Sweden do not have such general strict liability rules but provide for a series of specific strict liability statutes. All jurisdictions furthermore have special rules amounting to strict liability for damage caused to the neighbourhood by excessive polluting interference (England: private and public nuisance; France: 'troubles de voisinage' etc). Special strict liability regimes regulate third party liability for airplanes, genetically modified organisms, nuclear installations, medical products (pharmaceuticals) and environmental harm (see 4.3.1.3.2).

It is evident that these liability rules only apply to the operator of the activity and not to the security company that is hired by the operator to provide for security services. The security company is only liable according to the heads of liability applicable to it, which – under normal circumstances – is fault based liability (English law: negligence) and product liability (see above).

Multiple causation

If indivisible damage is caused by two or several tortfeasors, although by independent and separate acts, it is the general rule in all jurisdictions that the tortfeasors are jointly and severally liable. As a consequence, each tortfeasor can be sued by the victim for the entire sum of compensation. The tortfeasor who compensated the victim then has a right of recourse against the other contributors (see 4.3.4.1.). The decisive criteria for the assessment

288 France: Law no 98-389 from 19 mai 1998 which inserted the new section IV ‘de la responsabilité du fait des produits défectueux’ (C. civ., art. 1386-1 à 1386-18) into the Code civil; Germany: Produkthaftungsgesetz; Sweden: Produktansvarsregler (1992:18); UK: Consumer Protection Act 1987; Poland: Article 449-1-449-10 civil code; Spain: Law 23/1994 from 6 July 1994, de responsabilidad civil por los daños causados por productos defectuosos (LRPD) as revised by Royal Legislative Decree 1/2007 of 16 November 2007 por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLDCU).
of the shares of the contributors are quite different in the countries analysed. The apportionment may be carried out according to the seriousness of fault of each contributor, or simply per capita or according to the particular circumstances of the individual case.

The right of recourse applies to the client who compensated the victim for the loss incurred and vice versa to the security company if both client and security company are liable for the same damage. It must be borne in mind that the recourse between the client and the security company can be regulated by the contract concluded between both parties. It can be adjusted to the special circumstances of the situation and it is admissible that the client limits or completely renounces his right of recourse against the security provider.

4.4.3. Liability of the security provider for damage caused by a natural disaster or an act of terror

4.4.3.1. Negligence and fault based liability (Case 2)

The main head of liability for the security provider as regards third parties is the tort of negligence in the common law and fault based liability in civil law countries. Both liability regimes require causation and the establishment of a breach of a duty of care. Under negligence (common law) and fault based liability (civil law) the tortfeasor is only liable for harm that would not have occurred if the tortfeasor had not breached the duty of care. The security provider thus is not liable for unforeseeable harm or harm that would not have been prevented by reasonable safety precautions. The security provider must meet an objective standard according to its special knowledge and abilities (see 4.3.1.1.).

If the damage is caused by a natural disaster (Case 2: earthquake) or by an intentional act by a third party (Case 2: terrorist attack), the security provider will only be liable if he had a duty of care to prevent the occurrence of a specific type of damage in such a scenario. With respect to the client, the duty of care of the security provider will be specified by the contract. These contractual obligations govern the direct liability of the security provider for the damage sustained by the client himself and also in respect of the question if and to what extent the client will be able to seek recourse from the security provider (for compensation rendered to third parties according to the heads of liability that are applicable to the client). With respect to third parties, the question of whether the security provider owed them a duty of care or not must be assessed according to general tort law. For this assessment the contractual obligations of the security provider towards the client are very important, but not solely decisive (see above under 4.4.2.1.).

Under strict liability such events (natural disaster, terrorist attack) are qualified in most countries\(^{289}\) as a ‘force majeure’ or ‘act of god’ and may exonerate the person who is subject to the strict liability regime from liability. This, as most of the national reporters indicate in the answers to Case 2, will however only be the case if the event was of an external, unpredictable and irresistible character (French report) or, as defined by the German Bundesgerichtshof\(^{290}\) as cited in the German report, if the event was ‘an external incident caused by natural forces or by third party acts that cannot be foreseen and that cannot be avoided with reasonable cost and with utmost care and that also must not be accepted due to its frequent occurrence’. In the scenario at issue in this study, this defence applies not to the security provider, who usually is only under an obligation of fault based liability, but to the

\(^{289}\) An exception is Sweden.

\(^{290}\) See BGH, 23 October 1952, 7 BGHZ 338.
client. For the security provider it is only of importance for the recourse obligation towards the client.

4.4.3.2. Public service (infrastructure) undertaking (Case 3)

Case 3 explores the liability of the provider of security services in case of a terrorist attack against a public service (infrastructure) undertaking and the recourse option of the public service undertaking against the renderer of security services.

The question whether an infrastructure undertaking (waterworks of city B) or the security provider of the waterworks are liable for the poisoning of the water by a terrorist was answered very differently by the national reporters. In all the countries the water supplier is contractually liable to the consumers and, except in Sweden, the liability of the water supplier would require that the water supplier was at fault or vicariously liable for A.

Most reporters had serious doubts whether the security provider can be held directly liable by the victims of the attack. Only the reporter for England and Wales and the German reporter held A liable for the damage sustained by house owner D. The Dutch reporter saw only liability for the personal injury of D and the reporters from Spain, France, Poland and Sweden more or less clearly rejected A’s liability. In most countries there is no vicarious liability of the infrastructure undertaking for fault of the security provider who is regarded as an independent contractor either. Vicarious liability for the independent contractor is only recognised in German contract law and in the Netherlands. The Dutch reporter, however, like the Spanish reporter, came to the conclusion that water poisoning by a terrorist would be regarded as force majeure and the water supplier would thus not be contractually liable to the consumers. German law provides for special provisions for the public water supply and restricts compensation to personal injury and property damage. In France damage caused by terrorist acts is primarily borne by the Guarantee Fund for Victims of Terrorist Acts and other Offenses (FGTI). Only loss that is not covered by the Fund, namely property damage and pure economic loss, falls under the tort law system. The only country where the water supplier would be fully liable under strict liability is Sweden. Liability is regulated by the Environmental Code and covers personal injury and property damage. The fact that the damage was caused by an intentional act by a third party (the terrorist) does not exclude liability, as the defence of force majeure is not provided in the Environmental Code. The water supplier will have a right of contractual recourse against the security provider A.

Another head of liability would be product liability of the water works as water distributed by water works can certainly be regarded as a product in the sense of the product liability directive. Product liability only covers damages for personal injury and property.

The liability of the security provider for the costs of disaster relief measures taken by State E was denied by most reporters, although with different reasoning. In England and Wales the decisive reason is that such costs are regarded as pure economic loss which is not covered by the tort of negligence. For the French reporter there was no sufficient causal relationship, as the decision of State E to grant aid is a free choice that breaks the causal chain. For the Dutch, Polish and Swedish reporters the security provider will not be liable for such costs. According to the Spanish reporter, however, such costs are not excluded per se. Under the condition that fault of the security provider can be established, the liability of the security provider would also include such costs. German law would provide for a similar solution, although not under tort law but on the basis of negotiorum gestio.
4.4.3.3. Security services, border control (Case 4)

The goal of Case 4 was to explore liability of the public authority for defaults of the renderer of security services and the recourse option of the public authority. For all reporters it was quite difficult to establish the liability of State B or the security provider as there is no case law on this. The reporters from four jurisdictions (France, Germany, Poland and Sweden) are of the opinion that State E will not be liable according to tort law for damage incurred by a private person, caused by a terrorist who slipped through the border control and, consequently, there is no right of recourse against the renderer of the flawed security service. The reason is that the connection between the public duty of border control and the damage sustained is too loose. The French reporter discussed this notion with reference to the concept of causation, while the other reporters denied, or at least seriously doubted, that the public duty to control the border has the aim of protecting the individual citizen from a terrorist attack.

The other reporters came to the conclusion that there would be liability of the state if fault can be established and the damage was foreseeable (eg England and Wales, Netherlands, Spain). All reports have in common that there is no difference between the security consultant and the contractor for the video surveillance installation at the border crossing, except for the fact that the latter might rather be regarded as an independent contractor for whom the state would not be vicariously liable (see the Polish and the Spanish report).

4.4.3.4. Security services, airplane crash (Case 5)

Case 5 explores the liability of the renderer of airport security services in case of an airplane accident caused both by a careless passenger and a terrorist.

As outlined above in section 4.3.1.3.2, liability of the air carrier for damage caused to passengers is regulated by Reg 889/02. The air carrier is obliged to compensate passengers for death and bodily injury for up to 113,100 special drawing rights (SDR) subject only to the defence of contributory fault of the victim. For damage exceeding this cap, the air carrier is liable according to fault based liability with presumption of fault. The air carrier is exonerated if it proves that the damage was not due to the negligence or other wrongful act or omission of the carrier or its servants or agents, or that the damage was solely due to the negligence or other wrongful act or omission of a third party. Damage to persons other than passengers is regulated by national law.

The answers to Case 5 are much more straightforward than those to Cases 3 and 4. All the reporters, except the Swedish reporters, came to the conclusion that air carrier E can claim the costs of repairing the damaged airplane and the costs for the emergency landing from the security provider A under fault based liability (civil law) or negligence (common law), if the security provider negligently failed to detect the highly inflammable chemicals in the hand baggage of the passenger. In England and Wales the tort of negligence would also cover the damage claims of the injured passengers. The security provider owes a duty of care towards both plaintiffs, airline E and the passengers, because of the assumption of responsibility to prevent exactly such damage. Even the fact that the fire was started by the intentional act of a third party, namely the terrorist, would not exonerate the security provider from liability under English law. The liability of the security provider extends also to claims of third parties who sustain personal injury and property damage, if the airplane crashes, and the air carrier who is strictly liable for such damage under the Civil Aviation Act would have a right of full recourse against the security provider. In France the main question for the liability of the security provider is the requirement of a direct causal link between the act and the damage. For the damaged airplane, the cost of the emergency landing and the harmed passengers, the French reporter affirmed liability, as the security provider was expressly in charge to prevent
such damage, both in the case of the careless passenger and the terrorist. With respect to third parties harmed by an airplane crash caused by a terrorist, the causal link between the carelessness of the security provider and the damage, however, would be too remote. The French reporter hence denied direct liability of the security provider towards third parties and saw no room for an action of recourse by the liable airline against the security provider. If the damage was caused by a terrorist attack, the Guarantee Fund for Victims of Terrorist Acts and other Offenses (FGTI) would compensate the claims for personal injury. The Fund can then seek recourse from the airline and the security provider as far as they are liable.

In German law the security provider would be liable under fault-based liability of § 823 (1) BGB to the harmed passengers and to airline E in the case of the careless passenger. If the damage was caused by a terrorist the German reporter already hesitated to assume liability for the security provider as, according to tort law, it is the airline which is liable for damage to passengers. Liability for the airplane crash caused by a terrorist was frankly denied by the German reporter. Liability for such damage lies with the airline. Strict liability of the airline under § 33 Air Traffic Act (LuftVG) covers damage to persons and property up to a certain liability cap and there is no exception for terrorist attacks or force majeure in general. Airline E would have no recourse against the security provider, as there is no contract between the airline and the security provider and as the security provider is not liable for the damage.

In the Netherlands the security provider is liable under fault-based liability for the damage to the injured passengers and the damage incurred by the airline. Courts, however, may mitigate the compensation under Article 6:109 BW if the extent of the damages would be excessively burdensome for the security provider. In Dutch law the airline is not strictly liable for the damage caused to third parties by the aircraft. The Dutch reporters, however, assume that the security provider would be liable for the airplane crash caused by the terrorist. Again the reduction clause of Article 6:109 BW may be applied to reduce the liability burden.

In Poland the security provider would be liable under fault-based liability to the harmed passengers and to airline E when the damage was caused by the careless passenger, but not by a terrorist. The airline would have a right of recourse for damages paid to the passengers. For damage incurred by third parties the airline would be liable according to Articles 206-207 Aviation Law. If the damage is caused by a terrorist attack, liability is excluded and, hence, there is no recourse against the security provider. In Spain, like in all the other countries, the security provider would be liable under fault based liability for the damage incurred by airline E (damage to the airplane and the cost of the emergency landing), both in case of the careless passenger and the terrorist. For the damage sustained by the passengers liability lies with the airline. The airline is strictly liable for damage caused to third parties under the Act of Aeronautical Navigation (LNA) which does not provide for a defence when the damage was intentionally caused by a third party. The liability is limited in amount unless the operator of the aircraft acted with fault. The Spanish reporter saw also a good reason for state liability, as the security guards at airports act under the control and the orders of the public administration. For the Swedish reporters it is the airport operator and the police authority that are responsible for airport safety. Airline E can thus claim for the damage sustained (cost of repairing the airplane and cost of the emergency landing) according to contractual liability from airport B who then may take contractual recourse against the security provider A. Extra-contractual liability of the security provider could only be assumed if A acted with gross negligence or intent or, quite speculatively, if A breached a non-contractual duty to prevent damage to E. If A can be held extra-contractually liable to E, which is rather uncertain, then A will also be liable for damage caused by a terrorist, as Swedish law does not per se exclude liability for an intentional act by a third party. In the scenario of the airplane crash caused by the terrorist, liability would lie with airline E according to The Act on Liability for Damage Caused in the Course of Aviation. Direct liability of the security provider to third parties would require that the security provider owes the general public an extra-contractual duty to prevent damage, which the Swedish reporters seriously doubt.
4.5. Summary and conclusions

4.5.1. Case law

There is no special case law with respect to the third party liability of security companies in the jurisdictions analysed. Only the reporter for England and Wales referred to one case which, however, concerned the liability of the security company towards the client (Bailey v HSS Alarms), and the Swedish reporters cited a case which dealt with the right of recourse of the insurance company against the security company (NJA 2001, p. 711). The Swedish court rejected the claim with the reasoning that the breach of the contractual duties the security company owed to the client does not amount to negligence in tort towards the client’s customers.

4.5.2. Legislative limitations of liability

Legal channelling, liability caps and reduction clauses are instruments used by legislators to limit the liability of certain tortfeasors. Such instruments can be found in the jurisdictions analysed, but they are of an exceptional character.

4.5.2.1. Legal channeling

Legal channelling is an instrument typical for liability according to the international nuclear liability conventions (liability for oil pollution, where legal channelling also exists, was not mentioned in the national reports). In national tort law, legal channelling in the strict sense, meaning that it excludes liability of other tortfeasors (eg provider of products or services) and liability of the operator under other heads of liability, especially under fault based liability, is unknown. A certain degree of channelling is achieved by vicarious liability. No national law, however, totally excludes liability of the employee towards the third party and the right of recourse of the employer. Another example can be found in Sweden for the recourse of insurances with respect to property damage caused by someone’s employee (vicarious liability) or by the state or municipality. Legislative plans to channel liability for terrorist attacks to the state which were discussed in Sweden for some time have so far been rejected.

4.5.2.2. Liability caps

No country provides for a liability cap for fault based liability. In Germany liability caps are quite usual in strict liability statutes, but in the other countries liability caps are quite rare and mainly restricted to areas that are covered by international liability conventions.

4.5.2.3. Reduction clauses

Reduction clauses are not a common instrument for mitigating the liability of the tortfeasor. Only the Netherlands (6:109 BW) and Poland (Article 440 civil code; only for liability of natural persons) provide for such instruments, but the reporters write that this instrument is not widely used.
4.5.2.4. Other instruments

The Netherlands limit liability of particular providers of services (pilots, air traffic controllers) and of certain public authorities (Bank of Netherlands, Financial Markets Authority) to intentional, grossly negligent or wilfully reckless behaviour. When assessing such a legislative rule for the third party liability of the security provider one must take into account that the limitation of fault-based liability for personal injury and of compensation for property damage inflicted by gross negligence by contractual stipulation is problematic under aspects of fairness.\footnote{See section 4.3.5.2 above.}

4.5.3. Regulations for the security provider and their effect on tort liability

Security enterprises are often engaged in areas that are heavily regulated by public law. This applies to the operation of nuclear installations and airports as well as to industrial plants for the production of pharmaceuticals, genetically modified organisms or hazardous material. These rules are addressed to the operators of these activities. Security enterprises are only indirectly affected by them.

Rules regulating the activity of the security industry itself are comparatively rare (see 4.3.2.). Such rules can influence the tort liability of the security provider. The liability of the security provider is mainly determined by fault-based liability. In fault-based liability public law rules governing the behaviour of the security provider can affect the determination of the required standard of care. Regulation by public law will usually increase the required standard of care and thus tighten the liability obligations of the security enterprise. For courts the failure to comply with regulation is a strong indication that the defendant breached the required standard of care under tort liability. In several countries fault-based liability is aggravated in case of breach of a statutory rule with a protective scope (\textit{Schutzgesetz}). Compliance with public law standards, however, does not necessarily exempt from liability. In all the jurisdictions analysed, courts usually rely on such rules but do not feel bound by them. Standards set by courts according to the circumstances of the case can thus surpass the standards set by public law.

4.5.4. The liability risks of the security provider

The security provider is liable to the client for breach of the contract concluded. As a specialist and professional, the security provider must meet a high standard according to the special knowledge and abilities of the profession. He must inform the client of the available security measures, devices and achievable security standards and must warn the client of the risks should the client not opt for the best available solution. The same applies when the security provider takes note of this fact while performing the contract. If the contract specifies the type of measure, device or method that must be provided by the security provider, then the client cannot claim when harm occurs that the security provider should have taken another measure or should have used another device or method. Liability of the security provider can then only be established for the failure to adequately inform and warn the client.

The parties are free to shape the contents of the contract and can restrict the contractual liability of the security provider towards the client as well as the mutual recourse obligations of both parties. The contractual freedom is only limited by rules concerning the fairness of contractual clauses.
Towards **third parties**, the security provider is liable according to the rules of extra-contractual liability. There are two heads of liability available: fault-based liability and product liability, if the harm was caused by a product in the sense of the EU-product liability directive, which was produced and put into circulation by the security provider.

**Fault based liability** requires the breach of a duty of care. The wording and contents of the contract shape the potential liability of the security provider towards **third parties**. The contract not only defines the duties of the security provider, but also circumscribes to which persons the security provider owes a duty of care. The victim who is part of the protected group may sue the security provider directly for damages. With respect to third parties too, the security provider can in principle only be obliged to fulfil his contractual obligations. He cannot be held liable by the client or any third party for the fact that the stipulated measure, device or security standard does not meet the highest standard provided by the industry. Liability can only then arise if the security provider, who knew or should have known that the security measures are inadequate, failed to inform the client of this fact in order to enable the client to take measures to prevent the damage. If the security provider, however, contractually agrees to provide for the security of a facility or an activity in a comprehensive and independent way, the security provider will also assume the liability in torts towards third parties. In many countries this situation is described by the theory of the liability of the **independent contractor**.

The breach of a contractual duty does not automatically amount to tortious behaviour towards a third party. All the seven jurisdictions that were examined provide for specific concepts to restrict the responsibility of the tortfeasor for harm that is not reasonably foreseeable or too remote. These restrictions play an important role for the liability of the security provider for damage caused a natural disaster or by the intentional act of a third party (see 4.5.6.). They apply to all types of damage, but are quite essential in respect of the compensability of pure economic loss sustained by third parties.

In all jurisdictions fault based liability covers damages for personal injury, harm to property and consequential economic loss. Under extra-contractual liability, compensation for **pure economic loss** is rather restricted. In England and Wales, Germany and Sweden pure economic loss is only recoverable under exceptional circumstances. In the other countries (France, Netherlands, Poland and Spain), which do not distinguish between pure economic loss and the other heads of damage in the first place, the compensability of pure economic loss is restricted by further considerations, such as the necessity of a sufficiently direct causal link (France, Spain) or by the concept of adequacy (Poland) or by more general considerations (Netherlands).

The responsibility of the security provider will not usually extend to the compensation of **environmental damage** such as relief measures taken by a public entity, preventive measures by the public authority or remedial action, as the security provider is not liable according to the Environmental Liability Directive. The national rules for compensation of environmental damage are rather complex and diverse in the various jurisdictions.

If the damage is caused by a product that was produced and put into circulation by the security provider, liability is regulated according to the rules of **product liability** set out by the Product Liability Directive. Liability under the national laws implementing the product liability directive is irrespective of fault and covers compensation for damage caused by death and personal injury as well as damage to property intended for private use or consumption with a lower threshold of € 500. Liability does not cover the compensation of pure economic loss and environmental damage which does not constitute property damage. The decision whether liability includes the recovery of non-material damage (pain and suffering) is left to
the Member States (Article 9 Product Liability Directive). Recovery for non-material damage under product liability is provided by all of the jurisdictions analysed except for Spain.

If both the security provider and the client are liable for the same damage, joint and several liability applies. Each tortfeasor can be sued by the victim for the entire sum of compensation and the tortfeasor who compensated the victim has a right of recourse against the other contributor. The right of recourse can be regulated in the contract concluded between the client and the security provider and can be adjusted to the special circumstances of the situation.

4.5.5. Standard and burden of proof

The required standard of proof varies in the jurisdictions analysed. In England and Wales and the Netherlands the relevant standard of proof is the balance of probabilities. In the other countries facts must be established with high probability or even with certainty which means that the court must be convinced beyond reasonable doubt.

All the jurisdictions provide that in extra-contractual liability the burden of proof lies with the claimant. For fault based liability this applies to the proof of the damage sustained, fault and causation. Under product liability the injured person must prove damage, the defect in the product and the causal link between damage and defect. In all the countries analysed, courts have some discretion with respect to the establishment of fault and causation. Such discretion ranges from the doctrine of res ipsa loquitur or prima facie evidence for the proof of fault to complex strategies for the establishment of causation in cases of mere statistical evidence. Under certain circumstances the burden of proof may be shifted partly or entirely to the defendant. These strategies are often applied in medical malpractice or in environmental liability cases and have no specific relevance for the security industry.

All of the national legal systems analysed provide for special rules on case management, but none of the national legal systems analysed provides for a US-style class action.

4.5.6. Liability of the security provider for damage caused by a natural disaster or an act of terror

The main head of liability for the security provider towards third parties is fault based liability which requires the breach of a duty of care and the establishment of a causal link between the breach and the damage incurred. If the damage is caused by a natural disaster or by an intentional act of a third party, the security provider will only be liable if he had a duty of care to prevent the occurrence of such damage. With respect to the client, the duty of care of the security provider will be specified by the contract. These contractual obligations govern the direct liability of the security provider for the damage sustained by the client himself and also for the question of whether and to what extent the client will be able to seek recourse from the security provider for compensation rendered to third parties.

With respect to liability towards third parties, the question whether the security provider owes them a duty of care or not must be assessed according to general tort law. For this assessment the contractual obligations of the security provider towards the client are very important. Liability can only be imputed to the security provider if his contractual duties implied the

292 Eg the client under a strict liability regime and the security provider under fault-based liability, or both under fault-based liability for the breach of a duty of care they owed to the victim.
duty to prevent such damage. Even if the security provider assumed responsibility for the prevention of such damage in the contract, he may not be directly liable to third parties as the link between the carelessness of the security provider and the damage sustained may be assessed as too remote to trigger liability.

Under strict liability, such events (natural disaster, terrorist attack) are qualified in most countries as a ‘force majeure’ or ‘act of god’ and may exonerate the person who is subject to the strict liability regime from liability. This defence applies only to the client and not to the security provider, who usually is only under an obligation of fault based liability. For the security provider it is of indirect relevance, as there will be no recourse obligation towards the client, if the client is not liable.

Damage caused by terrorist attacks is often compensated by the state. In France, Spain and the UK special compensation schemes for victims of terrorism have been established. While the British compensation scheme only grants compensation to victims of terrorism who cannot obtain compensation from other sources, the French and the Spanish compensation schemes provide for subrogation.

4.6. Theses

The findings of this chapter can be summarized in the following theses:

1. There is no special case law with respect to the third party liability of security companies in the jurisdictions analysed (reported cases: England and Wales: Bailey v HSS Alarms, Sweden: NJA 2001, p 711).

2. Instruments to limit the liability of certain tortfeasors (legal channelling, liability caps, reduction clauses) can be found in the jurisdictions, but they are of an exceptional character. There is no tradition to limit fault-based liability.

3. Public law regulation of the security industry is rare. Public law rules may have the effect to clarify the duties of the security provider, but will usually tighten his liability obligations.

4. The liability of the security provider towards the client is regulated by the contract. The contractual freedom is only limited by rules concerning the fairness of contractual clauses. The contract is also essential for the recourse obligation of the security provider towards the client.

5. Liability for the secured activity towards third parties lies primarily with the client who is liable under fault-based liability or under various, rather inconsistent national rules on strict liability. Recourse of the client against the security provider is only possible, if the security provider himself is liable towards the third party (recourse under joint and several liability) or if recourse is provided by the contract.

6. Only if the security provider contractually agrees with the client to take over the whole responsibility to provide for the security of an activity or facility, he will assume an independent duty in tort to protect third parties from harm caused by this activity or facility (theory of the liability of the independent contractor). This liability is fault based and will not cover pure economic loss.

7. The security provider is not under an obligation of strict liability under national law. Applicable liability regimes are only fault-based liability or, for the producer of a security device, product liability.
8. **Fault-based liability** requires that the security provider breached a duty of care. These duties are defined by the contract concluded with the client. The security provider cannot be held liable by the client or any third party for the fact that the stipulated measure, device or security standard does not meet the highest standard provided by the industry. Liability can in this case only arise if the security provider, who knew or should have known that the security measures are inadequate, failed to inform the client of this fact.

9. In all jurisdictions fault-based liability covers **damage** for personal injury, harm to property and consequential economic loss. Compensation for pure economic loss and for environmental damage is rather restricted.

10. Liability under **product liability** is determined by the EU-product liability directive. Liability covers manufacturing, design and warning (marketing) defects. The product must meet an objective safety standard (according to technical standards etc) which, however, can, according to Article 6 (1) (a), be specified *inter alia* by the presentation of the product by the producer on the market (e.g. sales promotion, sales contract, instructions for installation and use). The producer of a security device will thus not be liable for the mere fact that another product on the market would have achieved a higher security standard. The exposure under European product liability law is limited to personal injury and property damage to private persons, excluding pure economic loss and punitive damage.

11. If harm is caused by a **natural disaster or by an intentional act of a third person**, the security provider will only be liable if he had a duty of care to prevent the occurrence of such damage. With respect to the client, the duty of care of the security provider will be specified by the contract. With respect to liability towards third persons, the question whether the security provider owes them a duty of care or not must be assessed according to general tort law. For this assessment the contractual obligations of the security provider towards the client are very important. Liability can only be imputed to the security provider if his contractual duties implied the prevention of such damage. Even when the security provider assessed responsibility for the prevention of such damage in the contract he may not be directly liable to third parties as the link between the carelessness of the security provider and the sustained damage may be assessed as too remote to trigger liability.

12. Under strict liability such events (natural disaster, terrorist attack) are in most countries qualified as ‘force majeure’ or ‘act of god’ and may exonerate the person who is subject to the strict liability regime from liability. This defence applies only to the client and not to the security provider, who is only under an obligation of fault based liability. For the security provider it is of indirect relevance, as there will be no recourse obligation towards the client, if the client is not liable.

13. Damage caused by terrorist attacks is often compensated by the state. In France, Spain and the UK special compensation schemes for victims of terrorism are established. While the British compensation scheme only grants compensation to victims of terrorism who cannot obtain compensation from other sources, the French and the Spanish compensation schemes provide for subrogation.

14. All of the national legal systems analysed provide for special rules on **case management**, but none of the systems provides for a US-style class action.
Chapter 5 Analysis of potential analogy bearing international law treaties on civil aviation, nuclear safety and environmental liability

In this chapter we will address analogies between on the one hand liability regulated in various treaties concerning civil aviation, nuclear safety and environmental matters and on the other hand potential third party liability for security related products and services. We will, like in chapters 3 and 4, have two main goals in mind. First we will examine to what extent the international treaties analysed in this chapter have some relevance for the security industry; second we will analyse whether the features of these liability regimes may be interesting to consider in a possible future liability regime for the EU security industry. We will in turn deal with treaties related to civil aviation (5.1), nuclear liability (5.2), environmental liability and more particularly marine oil pollution (5.3), and other relevant treaties (5.4).

5.1. Civil aviation

In this section, two Conventions will be discussed: the Rome Convention of 1952 (5.1.1) and the Montreal Convention of 1999 (5.1.2).

5.1.1. 1952 Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (Rome Convention)

5.1.1.1. Brief summary of the regime

The Rome Convention establishes a liability and compensation framework for damage caused by aircrafts to third parties on the surface. With the development of civil aviation, people started to realize the potential damage caused by aircrafts, to both the persons and property on board and to third parties on the surface. The Convention for the Unification of Certain Rules relating to International Carriage by Air was concluded in Warsaw in 1929, and applies to damage to international carriage of persons, baggage and cargo. Damage to third parties on the surface has a different characteristic, in that usually an ex ante contract cannot be reached between the potential injurers and victims. A separate liability regime was therefore established in 1952: the Rome Convention. This convention was later revised by the 1978 Protocol to Amend the Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (1978 Protocol). Another attempt was made to further revise the Convention and an outcome was reached in 2009: the 2009 Convention on Compensation for Damage Caused by Aircraft to Third Parties. However, this new convention has not come into force yet. Hence the analysis here focuses on the 1952 Rome Convention and its 1978 Protocol.

5.1.1.2. Basis of liability

Strict liability is established under the 1952 Rome Convention. Article 1 requires the victim only to prove that “the damage was caused by an aircraft in flight or by any person or thing falling there from”, but not the negligence of the injurer. In other words, the injurer is strictly liable, irrespective of whether a fault can be established or not. To establish liability, the

293 This corresponds to Work Package 3 from the Invitation to Tender.
Convention requires that the damage is a direct consequence of the incident. If the damage is caused by “the mere fact of passage of the aircraft through the airspace in conformity with existing air traffic regulations”, liability cannot be established.\(^\text{294}\)

### 5.1.1.3. Liable persons (attribution of liability)

The Rome Convention attributes liability to aircraft operators. The term “operator” is defined as “the person who was making use of the aircraft at the time the damage was caused, provided that if control of the navigation of the aircraft was retained by the person from whom the right to make use of the aircraft was derived, whether directly or indirectly, that person shall be considered the operator.”\(^\text{295}\) The registered owner can be regarded as the operator unless he proves that some other person was the operator.\(^\text{296}\) The 1978 Protocol further clarifies the situation for state-owned aircrafts. In those cases, the person to whom the aircraft has been entrusted for operation is the liable party.\(^\text{297}\)

With the exception of deliberate acts or omissions, Article 9 of the Convention constitutes the only basis of liability for the operators. However, this Convention does not expressly exclude liability of other parties and it does not prejudice the right of recourse against other parties (Article 10).

### 5.1.1.4. Damage covered

The Rome Convention has no provision that directly clarifies the scope of compensable damage. But when discussing the priority in awarding different types of damage, the Convention mentioned several titles: loss of life, personal injury and damage to property.\(^\text{298}\)

Liability caps are established under the Rome Convention according to the weight of the aircraft. They are defined as follows:\(^\text{299}\)

<table>
<thead>
<tr>
<th>Aircraft weighing less than (including) 1,000 kg</th>
<th>More than 1,000 and not exceeding 6,000 kg</th>
<th>More than 6,000 and not exceeding 20,000 kg</th>
<th>More than 20,000 and not exceeding 50,000 kg</th>
<th>Over 50,000 kg</th>
</tr>
</thead>
<tbody>
<tr>
<td>500,000 francs plus 4000 francs per kg over 1000 kg</td>
<td>2,500,000 francs plus 400 francs per kg over 6,000 kg</td>
<td>6,000,000 francs plus 150 francs per kg over 20,000 kg</td>
<td>10,500,000 francs plus 100 francs per kg over 50,000 kg</td>
<td></td>
</tr>
</tbody>
</table>

The Rome Convention also establishes a cap for loss of life or personal injury, which is capped at 500,000 francs per person killed or injured.\(^\text{300}\) Liable parties will lose their right of limitation if the damage is caused by the deliberate act or omission of the operator, his servants or agents (in the course of their employment and within the scope of their authority).

---

\(^{294}\) Article 1 of the 1952 Rome Convention.  
\(^{295}\) Article 2 (2a) of the 1952 Rome Convention.  
\(^{296}\) Article 2 (3) of the 1952 Rome Convention.  
\(^{297}\) Article II of the 1978 Protocol.  
\(^{298}\) Article 14 of the 1952 Rome Convention.  
\(^{299}\) Article 11 (1) of the 1952 Rome Convention.  
\(^{300}\) Article 11 (2) of the 1952 Rome Convention.
If a person wrongfully takes and makes use of an aircraft without the consent of the person entitled to use it, the former’s liability is also unlimited.\(^{301}\)

If the total claims exceed the limit of liability, a priority rule shall apply: (1) if the claims concern only death or personal injury or concern only property damage, such claims are reduced in proportion to their respective amounts; (2) if the claims concern both types of damage, one half of the total sum distributable shall be appropriated preferentially to meet claims in respect of loss of life and personal injury; the remainder shall be distributed proportionally among all the remaining claims.\(^{302}\)

The 1978 Protocol increased the liability caps as follows:

<table>
<thead>
<tr>
<th>Aircraft weighing 2,000 kg or less</th>
<th>More than 2,000 kg and not exceeding 6,000 kg</th>
<th>More than 6000 kg and not exceeding 30,000 kg</th>
<th>More than 30,000 kg</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 2,000 kg and not exceeding 6,000 kg</td>
<td>300,000 SDRs plus 175 SDRs per kg over 2,000 kg</td>
<td>1,000,000 SDRs plus 62.5 SDRs per kg over 6,000 kg</td>
<td>2,500,000 SDRs plus 65 SDRs per kg over 30,000 kg</td>
</tr>
</tbody>
</table>

The cap for loss of life/personal injury per person was increased to 125,000 SDRs (Special Drawing Rights).\(^{303}\) The priority rule in case the liability limit is exceeded was adapted as well: it remains the same when claims concern only one type of damage; if claims concern both personal injury and property damage, a priority is given to personal injury. Only if there is still a remainder after payment for personal injury, compensation will be made to property damage proportionately.\(^{304}\)

5.1.1.5. Exclusions and defences

The Rome Convention allows a very limited defence. Article 5 states that “[a]ny person who would otherwise be liable under the provisions of this Convention shall not be liable if the damage is the direct consequence of armed conflict or civil disturbance, or if such person has been deprived of the use of the aircraft by act of public authority”. The usual defences, such as natural disaster or acts of terrorism are not mentioned. Comparative negligence is established: if the damage is caused solely or partly by the victims or their servants/agents, liability can be exonerated or reduced. However, if the damage is caused by the negligence/deliberation of a servant or agent of the victim and the victim can prove that his servant or agent was acting outside the scope of his authority, liability cannot be exonerated or reduced.\(^{305}\)

5.1.1.6. Relationship with regulation

Article 1 of the Rome Convention contains a provision concerning the interaction between liability and regulation: “there shall be no right to compensation if the damage […] results from the mere fact of passage of the aircraft through the airspace in conformity with existing air traffic regulations”.

---

\(^{301}\) Article 12 of the 1952 Rome Convention.

\(^{302}\) Article 14 of the 1952 Rome Convention.

\(^{303}\) Article III of the 1978 Protocol.

\(^{304}\) Article IV of the 1978 Protocol.

\(^{305}\) Article 6 of the 1952 Rome Convention.
5.1.1.7. Financial security and compensation mechanisms

The Rome Convention establishes a mandatory financial security system. Any Contracting parties may require the aircraft operator to maintain insurance coverage for the liability for damage in its territory up to the liability limitation.\textsuperscript{306} The insurer needs to be authorized to effect such insurance under the law of the State where the aircraft is registered or the State of the insurer’s residence or principal place of business.\textsuperscript{307} In addition to insurance, operators can also use other financial security mechanisms, such as a cash deposit, bank guarantee or guarantee by the Contracting State where the aircraft is registered.\textsuperscript{308} The Rome Convention allows direct action by victims against the insurer or guarantor, if the guarantee is valid and the operator is bankrupt. However, this does not prejudice the law governing the contract of insurance/guarantee concerning the right of direct action.\textsuperscript{309}

5.1.1.8. Rules of evidence

In order to be entitled to compensation, the victim needs to prove that the damage was caused by an aircraft in flight or any person or thing falling there from.\textsuperscript{310} If the damage is caused solely or partly by the negligence or other wrongful act or omission of a servant or agent of the victim, to make the comparative negligence defense provision invalid, the victim needs to prove that his servant or agent was acting outside the scope of this authority.

Liability is capped under the Convention. The victims can benefit from unlimited liability if he can prove the damage is caused by a deliberate act or omission of the operator, his servants or agents.\textsuperscript{311}

5.1.1.9. Conclusions Rome Convention and Relevance to the Security Industry

The Rome Convention is relevant to the security industry. For example, damage may be caused by the failure of alarm or security measures aiming at the prevention of a terrorist attack or natural disaster.

According to the Convention, terrorisms or natural disasters cannot exonerate the operators from liability. Hence the security industry will not be held liable directly. However, recourse is still allowed under the Convention. The security industry could therefore be asked to pay in accordance with applicable law in addition to the Convention.

5.1.2. 1999 Convention for the Unification of Certain Rules for International Carriage by Air (Montreal Convention)

5.1.2.1. Brief summary of the regime

A liability regime for international carriage of persons, baggage or cargo was established in Warsaw in 1929, when commercial aviation was still in its infancy. Afterwards, a series of revisions were reached from the 1950s to the 1970s. With the development of civil aviation,
these instruments seem inappropriate to address the liability and compensation issues. Under the auspices of the International Civil Aviation Organization, a new convention was concluded to modernize and consolidate the Warsaw Convention and related instruments in Montreal in 1999: the Convention for the Unification of Certain Rules for International Carriage by Air (Montreal Convention). According to its Preamble, the Montreal Convention has two aims: to ensure the protection of an equitable compensation for consumers of international carriage by air and to promote the development of international air transport operation. It applies to international carriage of persons, baggage or cargo performed by aircraft. To satisfy the requirement of “international”, the places of departure and destination are either in different States Parties; or in the same State Party, but the agreed stopping place is in another State.\textsuperscript{312}

\subsection*{5.1.2.2. Basis of liability}

The Montreal Convention establishes three types of liability: liability for death and injury of passengers, damage to baggage and damage to cargo.

Strict liability is established for death and bodily injury of a passenger, if the damage happened on board the aircraft or in the course of embarking or disembarking. In case of destruction or loss of, or damage to baggage, the basis of liability depends on the checking status of the baggage. Strict liability applies for checked baggage. For unchecked baggage and personal items, the carrier is only liable if fault can be found for the carrier or its servants/agents.\textsuperscript{313} Strict liability is also established for the destruction or loss of, or damage to cargo, if it was caused during the carriage by air. The period of carriage by air does not include any carriage by land, by sea or by inland waterway performed outside an airport.\textsuperscript{314} The carrier is also liable for damage caused by delay in the carriage by air of passengers, baggage or cargo.\textsuperscript{315}

\subsection*{5.1.2.3. Liable persons (attribution of liability)}

Articles 17-19 of the Montreal Convention impose liability on air carriers. If the carriage by air is performed by another person rather than by the contracting carrier, both the contracting carrier and actual carrier shall be held liable: the former for the whole of the carriage contemplated in the contract and the latter solely for the carriage which it performs.\textsuperscript{316} Liability can also be addressed against the servants or agents of the contracting/actual carriers. The Convention does not prejudice the right of recourse against any other person.\textsuperscript{317}

\subsection*{5.1.2.4. Damage covered}

The Montreal Convention covers damage to passengers, baggage or cargo. It also applies to the delay in the carriage. Liability caps are established respectively for those types of damage.

The Carrier is liable for each passenger for death of injury of passengers up to 100,000 SDRs. For the amount in excess to 100,000 SDRs, the carrier can be exonerated from liability, if it

\textsuperscript{312} Article 1 of the Montreal Convention.
\textsuperscript{313} Article 17 of the Montreal Convention.
\textsuperscript{314} Article 18 of the Montreal Convention.
\textsuperscript{315} Article 19 of the Montreal Convention.
\textsuperscript{316} Article 40 of the Montreal Convention.
\textsuperscript{317} Article 37 of the Montreal Convention.
can prove that the damage was not due to the negligence or wrongful act or omission of the carrier or its servants/agents or the damage was solely due to the negligence or other wrongful act or omission of a third party. 318

For the damage caused by delay in the carriage of persons, the liability for each passenger is limited to 4,150 SDRs (Article 22 (1)). In case of the carriage of baggage, the liability cap for destruction, loss or delay is set at 1,000 SDRs per passenger, unless an ex ante declaration allowing higher compensation exists (Article 22 (2)). Similarly, for the carriage of cargo, the liability for destruction, loss or delay is limited to 17 SDRs per kg, unless an ex ante declaration allowing higher compensation exists (Article 22 (3)).

In case of the carriage of passengers and baggage, the carrier will lose its right to limit liability, if “the damage resulted from an act or omission of the carrier, its servants or agents, done with intent to cause damage or recklessly and with knowledge that damage would probably result; provided that, in the case of such act or omission of a servant or agent, it is also proved that such servant or agent was acting within the scope of its employment”.

According to Article 25 of the Montreal Convention, a higher liability cap or no liability is also allowed if the carriage contracts stipulate so.

5.1.2.5. Exclusions and defences

The Montreal Convention in Article 20 allows for a comparative negligence defence. If “the damage was caused or contributed to by the negligence or other wrongful act or omission of the person claiming compensation, or the person from whom he or she derives his or her rights”, the carrier’s liability can be exonerated or reduced.

For damage caused by delay, if the carrier can prove that it or its servants/agents took all measures that could reasonably be required to avoid the damage or that it was impossible to take such measures, he can be exonerated from liability. 320

5.1.2.6. Relation with regulation

The Montreal Convention does not only establish a liability framework but also contains some regulatory requirements, mainly concerning the documentation of the carriage. For example, in respect of carriage of passengers, the carrier shall provide a document containing the places of departure and destination; if the two places are in the same State, the stopping place in another State. For the carriage of baggage, an identification tag shall be provided to the passenger. The passenger shall be also informed with written notice about the limitation of liability. 321 Similar requirements apply to the carriage of cargo. 322 However, the Convention prescribes that non-compliance with these requirements shall not affect the validity of the contract of carriage which shall be subject to the rules of the convention, including the limitation of liability. 323

318 Article 21 of the Montreal Convention.
319 Articles 22 (5) of the Montreal Convention.
320 Article 19 of the Montreal Convention.
321 Article 3 of the Montreal Convention.
322 Article 4 of the Montreal Convention.
323 Articles 3 (5) and 9 of the Montreal Convention.
5.1.2.7. **Financial security and compensation mechanisms**

A mandatory insurance framework is established under Article 50 of the Montreal Convention. State Parties shall require their carriers to maintain adequate insurance coverage for their liability.

5.1.2.8. **Rules of evidence**

The Montreal Convention does not reverse the burden of proof and allows a presumption of liability generally. In order to make use of the comparative negligence provision, the carrier shall prove the negligence or wrongful act/omission of the victim or its servants/agents.\(^{324}\) As discussed earlier, in case of delay, the carrier needs to prove that it or its servants/agents took all measures that could reasonably be required to avoid the damage or that it was impossible for them to take such measures, in order not to be held liable.

As discussed above, the Convention also establishes a regulatory framework, which requires the carrier to provide the air waybill or cargo receipt in case of the carriage of cargo. The air waybill or cargo receipt is prima facie evidence of the conclusion of the contract, of the acceptance of the cargo and of the conditions of carriage mentioned therein. Its statement relating to the weight, dimensions and packing and the number of packages are also prima facie evidence.\(^{325}\)

5.1.2.9. **Conclusions Montreal Convention and relevance to the Security Industry**

Similar to the Rome Convention discussed previously, the Montreal Convention is relevant to the security industry in case of damage caused by the failure of alarming or security measures during a terrorist attack or natural disaster.

Again, terrorism and natural disasters are not valid defences, and air carriers are liable parties. Recourse against security companies is allowed. Hence the security industry could be asked to pay via recourse by the carriers.

5.2. **Nuclear liability**

5.2.1. **Origins and summary of the regimes**

5.2.1.1. **Origins of the nuclear liability regime**

At the beginning of the development of the nuclear industry, the Western-European market had to rely on American suppliers and technology. The American nuclear industry, however, was unwilling to bearing liability for possible nuclear accidents in Europe.\(^{326}\) Therefore, a “hold-harmless” clause was introduced in the first bilateral agreements between the US and the Europe, which required the European nuclear operators to indemnify the American suppliers for all claims resulting from their activities.\(^{327}\) Even with those “hold-harmless” clauses, the American industry was still unsure whether it could provide sufficient protection and the US “Atomic Industrial Forum” conducted a comprehensive study on the possibility of

---

\(^{324}\) Article 20 of the Montreal Convention.
\(^{325}\) Article 11 of the Montreal Convention.
\(^{326}\) See Vanden Borre 2007, p. 261-262.
\(^{327}\) Vanden Borre 2010, p. 180.
European victims claiming against American suppliers in case of a nuclear incident. Two reports were published later by the Atomic Industrial Forum: the “Preliminary Report on Financial Protection against Atomic Hazards” (the Preliminary Report”)

and the “International Problems of Financial Protection against Nuclear Risk” (“the Harvard Report”). Those two reports developed some principles for nuclear liability, which have been later incorporated into the international conventions.

The Preliminary Report identified four parties who can be affected by nuclear risks: the nuclear industry, private insurers, the government and the victims of a potential nuclear accident. In this report, the liability of the nuclear industry is linked with insurance capacity; for the part of damage that cannot be compensated by insurance, the government needs to provide additional compensation to protect the victims. The Preliminary Report introduced a system of unlimited government intervention: any damage in excess of the limitation of liable parties’ liability should be covered by the government in terms of indemnity.

The channelling of liability to nuclear operators was advised in the Harvard Report. According to the Harvard Report, the suppliers and contractors were exempted from liability for the following reasons: the suppliers are afraid of being held liable instead of or jointly with the operators and then being burdened by the lengthy trials; suppliers will lose control after the delivery of goods and services, and operators are more capable of obtaining insurance.

Those two reports proposed several principles for nuclear liability, which have later been adopted in a few national legislations and international conventions.

There are basically two types of nuclear liability conventions. The first type, often referred to as the first generation nuclear liability conventions emerged in the 1960s under the auspices of two international organisations. After the Chernobyl incident on 26 April 1986 new international conventions emerged which are referred to as the second generation of nuclear liability conventions. In addition specific conventions applied to the operators of nuclear ships and to the maritime carriage of nuclear material. Those different sets of conventions will be briefly presented. However, since the principles underlying these international nuclear liability conventions are very similar they can be discussed in an integrated manner. To the extent that there are differences between the conventions or protocols this will be indicated where needed.

5.2.1.2. First generation nuclear liability conventions

In 1960s, two international compensation regimes have been established for nuclear damage: the OECD regime and the International Atomic Energy Agency (IAEA) regime. Under the auspices of the OECD Nuclear Energy Agency (NEA), the Convention on Third Party Liability in the Field of Nuclear Energy of 29 July 1960 (Paris Convention) and the Brussels Supplementary Convention to the Paris Convention on Third Party Liability in the Field of Nuclear Energy of 31 January 1963 (Brussels Supplementary Convention) have been developed. The second regime was developed under the aegis of IAEA: the Vienna
Convention on Civil Liability for Nuclear Damage of 21 May 1963 (Vienna Convention). Those two regimes are usually called the first generation of nuclear liability conventions. Those two regimes have on the one hand, made an effort in establishing international/regional regimes for nuclear liability and on the other hand, have obvious limitations in terms of restricted geographical scope, narrow definition of nuclear damage and insufficient amount of available compensation.

Since the Paris Convention and the Brussels Convention are established under the auspices of the OECD/NEA, they are regionally confined to Western Europe, Slovenia and Turkey. The Vienna Convention, under the aegis of the IAEA is worldwide in scope. A few principles proposed in the Preliminary Report and in the Harvard Report were accepted under those two conventions.

According to the Paris Convention, the nuclear operator is liable for “damage to or loss of life of any person” and “damage to or loss of any property other than” onsite damage or property used in connection with the installations.

5.2.1.3. Second generation nuclear liability conventions

The Chernobyl accident in 1986 has triggered the intensive discussion about those limitations and later a revision process of the existing regimes was initiated. The so-called second generation of nuclear liability conventions was established thereafter. Those conventions consist of the Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention (Joint Protocol), the Protocol to Amend the 1963 Vienna Convention on Civil Liability for Nuclear Damage (the Protocol to the Vienna Convention), the Convention on Supplementary Compensation for Nuclear Damage (CSC), the Protocol to amend the Convention on Third Party Liability in the Field of Nuclear Energy of 29 July 1960 (the Protocol to the Paris Convention) and the Protocol to amend the Convention of 31 January 1963 supplementary to the Convention of 29 July 1960 on Third Party Liability in the Field of Nuclear Energy (the Protocol to the Brussels Supplementary Convention).

One has to understand this second generation nuclear liability conventions in the particular context within which the Chernobyl accident of 26 April 1986 occurred. The Chernobyl accident led to serious damage to human health, property and the environment with a broad transboundary impact. However, at that moment, the Soviet Union had no national legislation on nuclear liability. Nor was it a member of any international nuclear liability regimes. Even if the Soviet Union had joined the Vienna Convention, serious problems still prevent an effective compensation: the authorities in the Soviet Union questioned the necessity of the

---

336 See Vanden Borre 2010, p. 192.
337 Article III(a), the Paris Convention.
339 Vienna Convention as Amended by the Protocol of 12 September 1997 to Amend the Vienna Convention on Civil Liability for Nuclear Damage (the Protocol to the Vienna Convention).
340 Convention on Supplementary Compensation for Nuclear Damage (CSC).
preventive measures; the cap on liability under the Vienna Convention was dwarfed by the serious damage it caused; western European countries joined another regime which is independent of the Vienna Convention.

The lack of the acceptance of the international regimes and the insufficient resources available in case of a nuclear damage triggered the effort to revise the conventions. Another five conventions have been passed after the Chernobyl accident. The first effort was made to link the geographical scope of the existing regimes. In 1988, the Joint Protocol was adopted, under which, the operator of a nuclear installation situated in the territory of a party to one convention shall be liable for the nuclear damage suffered in the territory of a party to either the Paris Convention or the Vienna Convention. It was believed that the Joint Protocol would give incentives for the Central and Eastern Europe countries to join the Vienna Convention and would broaden the application of the two regimes. However, only 12 of the 18 countries in these areas which have joined the Vienna Convention became a member of the Joint Protocol. Globally, of the 52 States Party to the Paris and Vienna Conventions, only 27 Parties have joined the Joint Protocol.

In addition to the geographic links, some substantive changes were also adopted in the following years. Under the auspices of the IAEA regimes, two nuclear conventions were open for signature in 1997: the Protocol to the Vienna Convention and a stand-alone convention—the CSC. The CSC was made open to more countries: it maintains the essential principles established under the Paris Convention and tries to establish two tiers of public funds in case of nuclear damage. It is open to any state, if it is a party to either the Paris Convention or the Vienna Convention, or if it has national legislation containing the same principles. An effort was also made to revise the NEA conventions. In 2004, the Protocol to the Paris Convention and the Protocol to the Brussels Supplementary Convention were open for signature.

These new conventions and protocols are designed to overcome the deficiency of the first generation of nuclear liability conventions. However, the revisions have made eight international conventions available for nuclear liability, which lead to the so called a “labyrinth of international conventions” dealing with nuclear liability issues. Moreover, among the five new conventions, only two have come into force: the Joint Protocol entered into force in 1992 and the Protocol to the Vienna Convention came into force in 2003. Until now, only 5 countries have ratified the protocol to the Vienna Convention: Argentina, Belarus, Latvia, Morocco and Romania, and none of them have a significant nuclear generating capacity. There are still many large nuclear generating countries which are not a member of any of those conventions, such as the US, Canada, Japan, China, Korea, Russia, South Africa and Switzerland.

5.2.1.4. Maritime nuclear liability conventions

There are a few conventions that are less discussed in the literature since the literature mostly focuses on nuclear accidents in land-based facilities. There is also a convention on the

---

343 See Vanden Borre 2010, p. 192.
344 Article II, the Joint Protocol.
345 For the patchy and complicated approach under international nuclear liability conventions, see Currie 2008.
346 Of these five countries, only Argentina and Romania have nuclear capacity. The net nuclear power generating capacity of Argentina is 935 MWe and that of Romania is 1300 MWe in 2009. See Schwartz 2009.
liability of operators of nuclear ships of Brussels of 25 May 1962\textsuperscript{347} as well as a convention addressing nuclear liability issues in case of maritime transport.\textsuperscript{348}

These conventions carry largely similar principles as those included in the conventions dealing with land-based nuclear accidents, discussed before. Article II(1) of the Convention on the Liability of Operators of Nuclear Ships for example provides that the operator of a nuclear ship shall be “absolutely” liable for any nuclear damage upon proof that such damage has been caused by a nuclear incident involving the nuclear fuel of, or radioactive products or waste produced in, such ship. The liability of the operator of the ship is also capped and the operator is required to maintain insurance or financial security covering his liability for nuclear damage.

The goal of the Brussels Convention of 17 December 1971 relating to civil liability in the field of maritime carriage of nuclear liability is slightly different. It holds in Article 1 that any person who by virtue of an international convention or national law applicable in the field of maritime transport might be held liable for damage caused by a nuclear incident shall be exonerated from such liability if the operator of a nuclear installation is liable for such damage under either the Paris or the Vienna Convention or if the operator of a nuclear installation is liable for such damage by virtue of a national law governing the liability for such damage.

This hence means that the only goal of this convention is to provide exoneration from liability to any person who could be held liable in the field of maritime transport. This maritime transport convention of 1971 hence confirms the channelling of liability to the operator and is hence less interesting for the purposes of this study.

5.2.2. Basis of liability

A system of absolute liability is established under the Paris Convention.\textsuperscript{349} According to the Paris Convention, the operator is liable for damage caused by a nuclear incident in a nuclear installation or involving nuclear substances coming from such installations.\textsuperscript{350} To prove the fault of nuclear operators is no longer necessary to establish liability. Liability established under the Paris Convention is quite stringent since many classical exonerations, such as force majeure, Acts of Gods or intervening acts of third persons under general tort law are no longer applicable.\textsuperscript{351} The available exonerations are an act of armed conflict hostilities, civil war, and insurrection. The operator is not liable for damage caused via a grave natural disaster of an exceptional character unless the legislation of the Contracting Party in whose territory his nuclear installation is situated provides to the contrary.\textsuperscript{352} Similar stipulations about absolute liability and exonerations can also be found under the Vienna Convention.\textsuperscript{353} However, under the Vienna Convention, there is an additional possibility for operators to be relieved of his liability: the competent court can, according to the applicable law, relieve the operator wholly or partly from his obligation if the operator can prove that damage resulted from gross negligence or an act or the omission of the victims.\textsuperscript{354}
The conventions of the second generation have not changed the principle that strict liability is imposed on the operator of a nuclear power plant. However, an important change took place as far as the available defences for the operator are concerned: natural disasters are no longer an applicable defence.\(^{355}\)

Also the convention on the liability of operators of nuclear ships of 25 May 1962 provides that the operator of a nuclear ship shall be “absolutely liable”.\(^{356}\)

**5.2.3. Liable persons**

Under the Paris Convention, liability is channelled to operators. No one else is liable for the damage caused by a nuclear incident.\(^{357}\) The “operator” is defined as “the person designated or recognized by the competent public authority as the operator of that installation”.\(^{358}\) These provisions can hold other parties engaged in nuclear activities liable since the Paris Convention is the only legal basis for a claim against a nuclear operator in case of the identified incidents.\(^{359}\) This concentration of liability is based on two reasons: to avoid the complicated legal procedures to identify the liable parties and to allow a concentration of insurance capacity.\(^{360}\) Under the Paris Convention, the operators in principle do not have a right of recourse against the other parties. This is because it is argued that allowing recourse will make it necessary for suppliers to seek insurance coverage and will lead to costly duplication of insurance.\(^{361}\) However, recourse is possible if the damage results from an act or omission done with intent to cause damage or if and to the extent provided by contract.\(^{362}\) The Vienna Convention also has similar provisions.\(^{363}\)

Again, this principle of channelling liability exclusively to the nuclear operator can also be found in the second generation nuclear liability conventions as well as in the convention on the liability of operators of nuclear ships. The latter convention even explicitly holds “except as otherwise provided in this convention no person other than the operator shall be liable for such damage”.\(^{364}\)

This channelling of liability has quite some relevance for operators in the nuclear security industry. It means effectively that only the operator of a nuclear power plant will be held liable for a nuclear incident and that hence the security industry can in principle not be held liable for the damage caused as a result of nuclear accident, even if the nuclear accident would hypothetically have been caused by negligence on the side of the security industry. From the perspective of the security industry an exclusive channelling of liability to the operator of the nuclear power plant hence has the advantage that this basically excludes the possible liability of the security industry.

\(^{355}\) See Article IX, The Protocol to the Paris Convention; Article IV(3), The Protocol to the Vienna Convention.  
\(^{356}\) Article II(1) of the Brussels Convention on the Liability of Operators of Nuclear Ships.  
\(^{357}\) Article VI(a)(b), the Paris Convention.  
\(^{358}\) Article I(a)(vi), the Paris Convention.  
\(^{359}\) Article VI(c)(ii), the Paris Convention.  
\(^{360}\) The expose des motifs of the Paris Convention, point 15.  
\(^{361}\) The expose des motifs of the Paris Convention, point 18.  
\(^{362}\) Article VI(f), the Paris Convention.  
\(^{363}\) Article II(5), X, the Vienna Convention.  
\(^{364}\) Limited rights of recourse are allowed under Article II(6) of the Convention on the Liability of Operators of Nuclear Ships.
5.2.4. Damage covered

With respect to the type of damage that is covered and the amount there are two separate issues that deserve attention as far as the nuclear liability conventions is concerned. One specific aspect is that the liability of the nuclear power plant operator is seriously limited; another aspect relates to the heads of damage covered under the nuclear liability conventions.

5.2.4.1. Limitation of liability

Under both the Paris Convention and the Vienna Convention, the operator’s liability is limited both in amount and in time. The Paris Convention sets the maximum liability of the operator at 15 million SDRs, but allows the Contracting Party to establish by legislation a greater or lesser amount considering the capacity of insurance and financial security. The Contracting Party can also require a lower amount according to the nature of the installation. The lower amount should be no less than 5 million SDRs. The Paris Convention introduces a cap on liability, taking into account the difficulties of operators to seek financial security. The flexible expression allows the Contracting Parties to set the limit higher than that set in the Paris Convention. For example, in Sweden, the limit on liability is set at 300 million SDRs according to the Nuclear Liability Act (SFS 1968:45). Germany even adopted a system with unlimited liability. Under the Vienna Convention, the cap of liability should be no less than US $ 5 million. The statute of limitations under both the Paris Convention and the Vienna Convention is set at ten years from the date of the nuclear accident. They both allow the extension of the extinction periods by Contracting Parties if the operator is covered by insurance or other financial security.

The liability limitation has, however, been changed under the second generation nuclear conventions. The Protocol to the Paris Convention increases the limit for nuclear operators to be no less than 700 million euro. The Contracting party can reduce the liability to be no less than 70 million euro for an incident originating from a nuclear installation, or to be no less than 80 million euro for the carriage of nuclear substances according to the reduced risks. The Convention even allows the adoption of unlimited liability by the Contracting Parties, as long as the financial security required is no less than the amount mentioned above.

As already mentioned also in the convention on the liability of operators of nuclear ships the liability of the operator is limited to 1500 million francs in respect of anyone nuclear incident.

---

365 Article VII(b), the Paris Convention.
366 The expose des motifs of the Paris Convention, point 43.
369 Article V, the Vienna Convention.
370 Article VIII, the Paris Convention; Article VI(1), the Vienna Convention.
371 Article VII(a)(b), the Protocol to the Paris Convention.
372 Article X(b), the Protocol to the Paris Convention.
5.2.4.2. **Damage covered**

According to the Paris Convention, the nuclear operator is liable for “damage to or loss of life of any person” and “damage to or loss of any property other than” onsite damage or property used in connection with the installations.\(^{374}\) The Convention does not explain the two headings of damage further. What should be considered as damage to persons or damage to property is left to the discretion of competent court in accordance with the applicable national law.\(^ {375}\) Those two headings are also recognized as “nuclear damage” under the Vienna Convention. In addition to those two headings, “nuclear damage” under the Vienna Convention also includes “any other loss or damage so arising or resulting if and to the extent that the law of the competent court so provides.”\(^ {376}\) Therefore, more discretion is given to the competent court.

An important change made in the second generation conventions (both the NEA and IAEA regimes) is that the scope of nuclear damage has been broadened. Under the Protocol to the Paris Convention, in addition to personal injury and property damage, four new titles have been added to the concept of “nuclear damage”: the economic loss arising from personal injury and property damage; the costs of measures of reinstatement of the impaired environment; the loss of income deriving from a direct economic interest in any use or enjoyment of the environment, and the costs of preventive measures.\(^ {377}\) Similar provisions can also be found in the Protocol to the Vienna Convention. The difference is that under the latter, the definition of nuclear damage is open: it admits any other economic loss which is permitted by the general civil liability law in the competent court.\(^ {378}\)

The Convention on the Liability of Operators of Nuclear Ships of 25 May 1962 defines nuclear damage as

> “loss of life or personal injury and loss or damage to property which arises out of or results from the radioactive properties or a combination of radioactive properties with toxic, explosive or other hazardous properties of nuclear fuel or of radioactive products or waste; any other loss, damage or expense so arising or resulting shall be included only if and to the extent that the applicable national law so provides”.

5.2.5. **Exclusions and defences**

This issue has in fact already been dealt with when we discussed the scope of liability above (see 5.2.2). Summarizing, already under the first generation conventions, more particularly under the Paris Convention classic exonerations such as force majeure or the intervention of a third person were no longer available, but the operator was not liable for damage caused by a grave natural disaster of an exceptional character. However, that exception was also eliminated under the second generation international conventions: natural disasters are no longer an applicable defence.\(^ {379}\)

---

\(^{374}\) Article III(a), the Paris Convention.

\(^{375}\) The expose des motifs of the Paris Convention, point 39.

\(^{376}\) Article I(k), the Vienna Convention.

\(^{377}\) Article I(vii), the Protocol to the Paris Convention.

\(^{378}\) Article I(k), the Protocol to the Vienna Convention.

\(^{379}\) Article IX, The Protocol to the Paris Convention; Article IV(3), The Protocol to the Vienna Convention.
5.2.6. Causation

It may be surprising but none of the conventions discussed so far explicitly mentions the causation issue. This is indeed to some extent surprising since causation, especially in case of personal injury, may not always be easy to prove. For example, Article III(a)(2) simply mentions that the operator of a nuclear installation shall be liable for any property on that same site which is used or to be used in connection with any such installation “upon proof that such damage or loss was caused by a nuclear incident in such installation”. But there is no indication of how causation shall be proven. The only issue mentioned is where more than one party would cause the loss. In that case Article III(b) of the Paris Convention holds that where the damage or loss is caused jointly by a nuclear incident and by an incident other than a nuclear incident, that part of the damage or loss which is caused by such other incident, shall, to the extent that it is not reasonably separable from the damage or loss caused by the nuclear incident, be considered to be damage caused by the nuclear incident. If however the damage gives rise to liability of more than one operator in accordance with this convention the liability of these operators shall be joint and several.380 Also the Vienna Convention simply holds that the operator of a nuclear installation shall be liable for nuclear damage upon proof that such damage has been “caused” by a nuclear incident.381 Similar language is used in the Convention on the Liability of Operators of Nuclear Ships of 25 May 1962, which requires that “such damage has been caused by a nuclear incident”.382 Hence all conventions explicitly require causation, but none of the conventions defines how causation should be determined or how the judiciary should deal for example with problems of causal uncertainty.

5.2.7. Relation with regulation

In this respect we can be short: there is, to put it simple, no relationship between the nuclear liability conventions and (compliance with or breach of) regulation. The reason is that the conventions all impose strict liability (in the terms of the conventions even absolute liability) on operators of nuclear facilities. This liability applies even when operators would have complied with all regulatory standards; on the other hand, a breach of a regulatory standard is also not a condition for liability. This is a consequence of the concept of absolute liability in the international nuclear liability conventions, as a result of which regulation has no influence on the scope of liability.

5.2.8. Financial security and compensation mechanisms

These two important issues should be discussed separately. On the one hand the operator is obliged to seek financial security (like insurance) to cover his liability; on the other hand, even though the liability of the operator is limited additional funding mechanisms apply, largely based on public funding.

5.2.8.1. Financial security

To seek financial security coverage for the operator’s liability is important for the international regimes on nuclear liability. Both conventions require the operator to have and maintain insurance or other financial security up to the cap of its liability.383 Insurance is the

380 See Article V(d) of the Paris Convention.
381 Article II(1) of the Vienna Convention.
382 Article II(1) of the Convention on the Liability of Operators of Nuclear Ships.
383 Article X, the Paris Convention; Article VII, the Vienna Convention.
most popularly used instrument for an operator to cover its liability. In fact, the cap on liability is usually set as the maximum available amount from the insurance market. Since insurance is available per installation for a fixed period rather than in respect of a single incident, the potential resources available for compensation may be reduced after the first incident. Under these conditions, the Contracting Parties may need to intervene.\textsuperscript{384} It is for the Contracting Parties to decide the nature, form and extent of the compensation according to applicable national law.\textsuperscript{385}

This obligation to seek financial security has not been changed in the second generation nuclear conventions. The obligation to provide security for the limited liability of the operator can also be found in the Convention on the Liability of Operators of Nuclear Ships.\textsuperscript{386}

5.2.8.2. Additional funding

The liability limits established under the Paris Convention and the Vienna Convention are quite low compared to the potential catastrophic damage that a nuclear incident can cause. The liability is limited to promote the development of the peaceful use of nuclear liability. To provide the potential victims better protection, the Brussels Complementary Convention was established under the auspices of the NEA in 1963. Under the Brussels Complementary Convention, two additional layers of compensation are added in terms of public funds. Therefore, the total amount of money available for compensation is increased to 300 million SDR, and a third layer compensation system is established: firstly, the operator is liable up to an amount of at least 5 million SDRs via its financial security; between this amount and 175 million SDR, the Installation State needs to make public funds available; for the amount between 175 and 300 million SDR, compensation is made out of public funds by all Contracting Parties according to a specific formula.\textsuperscript{387} The Installation State can escape its obligation under the second layer by setting the liability limit at no less than 175 million SDRs. In that case the whole amount up to 175 million SDR needs to be made available by liable operators.

This system of a three-tier of compensation has also been changed under the second generation nuclear liability conventions. Not only has the amount of the limitation of liability been increased;\textsuperscript{388} also the available public funds were increased. From the maximum amount of operators’ liability set by the Protocol to the Paris Convention up to 1200 million euro, the Installation State needs to pay in terms of public funds. Public funds need to be made available by all Contracting Parties according to a set formula of compensation between the amounts of 1200 million euro and 1500 million euro.\textsuperscript{389} Thus the available resources for compensation in case of a nuclear accident are increased significantly: from 300 million SDRs (approximately 327 million euro) to 1500 million euro.

The compensation capacity also increased under the IAEA regime. The Protocol to the Vienna Convention increases the liability limitation to no less than 300 million SDRs, or no less than 150 million SDRs, provided the Installation State will make public funds available to cover the amount between the set the limitation to 300 million SDRs.\textsuperscript{390} Thus the revision has introduced a second layer of compensation. Though the amount is also significantly

\textsuperscript{384} The exposé des motifs of the Paris Convention, point 49.
\textsuperscript{385} Article XI, the Paris Convention; Article VIII, the Vienna Convention.
\textsuperscript{386} Article III(2) of the Convention on the Liability of Operators of Nuclear Ships.
\textsuperscript{387} Article III(a)(b), the Brussels Complementary Convention.
\textsuperscript{388} See supra 5.2.4.1.
\textsuperscript{389} Article III(b), the Protocol to the Brussels Complementary Convention.
\textsuperscript{390} Article V(1), the Protocol to the Vienna Convention.
increased, it is modest compared to the possible significant damage and it is just set at the same level as the original Paris Convention and the Brussels Supplementary Convention. The CSC Convention also provides two tiers of compensation: a first 300 million SDRs is paid by public funds from the Installation State and another 300 million SDRs from the collective funds from the Contracting Parties.  

The result is hence that under the international liability conventions a substantial part of the compensation is not paid by the liable operator but via public funding. Limited public funding is also provided for in the Convention on the Liability of Operators of Nuclear Ships. Article XI(1) provides the possibility for the operator to constitute a so-called limitation fund in respect of any nuclear accident. However, Article XI(6) holds that where no fund has been constituted the licensing state shall adopt such measures as are necessary to insure that adequate sums provided by it or by insurance or other financial security shall be available. This article hence makes the state the guarantor of the limited liability of the operator under Article III. However, under this Convention on the Liability of Operators of Nuclear Ships the state does not provide funds in addition to the limited liability of the operator of the ship.

The amount of compensation under the Paris and Brussels Conventions can hence be summarized in the following table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator’s liability cap</td>
<td>91</td>
<td>700</td>
</tr>
<tr>
<td>State intervention</td>
<td>140</td>
<td>500</td>
</tr>
<tr>
<td>Contracting parties’ coverage</td>
<td>150</td>
<td>300</td>
</tr>
<tr>
<td>Total</td>
<td>381</td>
<td>1500</td>
</tr>
</tbody>
</table>

Note, however, that the Convention on Supplementary Compensation has not entered into force yet. Hence, the “old” amounts from the first column still apply.

5.2.9. Rules of evidence

In this respect we can refer to the discussion relating to causation. Also with respect to evidence there are no specific rules provided for in the conventions. Hence, general principles apply. Since, as mentioned above the conventions all require “causation” between the damage suffered by the victim and the nuclear accident the burden of proving causation in principle lays with the victim. The conventions themselves do not refer to presumptions concerning the causal link or to a shift of the burden of proving causation.

5.2.10. Jurisdictional and procedural issues

There are several procedural issues with respect to the nuclear liability conventions.

A first question that arises relates to the geographical scope of the conventions. The Paris Convention does not apply to “nuclear incidents occurring in the territory of non-Contracting States or to damage suffered in such territory unless otherwise provided by the legislation of the Contracting Party in whose territory the nuclear installation of the operator liable is

---

391 Article III(1), IV(1), the CSC Convention.
392 See 5.2.6.
The geographical scope of the Vienna Convention is less clear. Some argue that since the convention itself is silent on its geographical scope, the Vienna Convention on the Law of Treaties will apply. The convention applies to damage occurring in the territory of a State Party, on board aircraft registers in that state and on ships flying its flag. While others deduce from the article about the competent court that the geographical scope depends on the competent court and thus damage resulting from non-Vienna states could be covered by Vienna Convention.

As we explained above, the second generation nuclear liability conventions and more particularly the joint protocol has broadened the scope of application of the conventions. Under this joint protocol the operator of a nuclear installation situated in the territory of a party to one convention shall be liable for the nuclear damage suffered in the territory of a party to either the Paris Convention or the Vienna Convention. The Protocols are also designed to be attractive by broadening the applicable geographical scope. The Protocol to the Vienna Convention applies to nuclear damage wherever suffered, with a permitted exclusion if a non-contract party has nuclear installations but does not offer reciprocal benefits. The Protocol to the Paris Convention also covers damage suffered in some non-Contracting Parties which satisfy some specific requirements.

A second jurisdictional aspect is that both the Paris Convention and the Vienna Convention have an “exclusive jurisdiction” clause: the jurisdiction lies only with the courts of the Contracting Party within whose territory the nuclear incident occurred. If the nuclear accident happens outside the Contracting Parties’ territory or the place can not be determined, the jurisdiction lies with the courts of the Installation State of the liable operator. Since nuclear damage may have a transboundary effect, the exclusive jurisdiction can ensure that the cap of liability is not exceeded and that a fair distribution of compensation takes place, if the claims lead to insoluble problems.

A third jurisdictional aspect relates to the statute of limitations. Since the health impact of nuclear radiation may not manifest itself after decades, the revised conventions also extend the statute of limitation for claims for personal injury and death. Those kinds of claims need to be brought within 30 years from the date of the accident.

5.2.11. Conclusions Nuclear Liability and relevance to the security industry

Potentially, the security industry could be involved in protecting nuclear installations, either with security products or services. Moreover, nuclear installations could potentially be a target of terrorist activities. However, the channelling of liability to the operator means that only the operator of the nuclear installation is held liable under the nuclear liability conventions discussed in this section. This channelling hence provides full protection to the
security industry which can, at least under the nuclear liability conventions, not be held liable for damage resulting from a nuclear accident.\textsuperscript{403}

Another issue is whether the nuclear liability conventions could constitute an example for an optimal liability regime for the EU security industry. Admittedly, the regime concerning the liability of nuclear operators is favourable for nuclear operators: liability is strict and channelled, but liability is limited and moreover a financial cap on the liability of the nuclear operator applies as a result of which the operator is not fully exposed to liability. Public funds are made available to cover the damage above the amount of the operator’s cap. At the time when the original conventions were made in the 1960s this arrangement (a low financial cap protecting the operator with public funding) was considered necessary to stimulate the newly emerging nuclear industry. In that sense a parallel with the security industry would be possible to the extent that the security industry would (like the nuclear sector in the 1960s) also have to be considered as a new and upcoming sector which could not develop without a financial limit on liability and public support to cover remaining damage. This is an important policy (and political) issue to which we will formulate some observations in Chapter 8.

At this stage it is, however, already important to mention that the nuclear liability regime as developed via the international conventions has received some criticism in legal doctrine. First, there is criticism on the limitation on the liability of the licensee of the nuclear power plant. The cap of liability puts potential victims in an unfavourable position. Moreover, under the strict liability regime, liable parties will only have incentives to prevent damage to the extent of the cap. Underdeterrence may lead to a less efficient care level. Under the original Conventions, the cap was set as 15 million SDR or $5 million. The amount was substantially increased in the Protocols, to be no less than 700 million Euro or 150 million SDRs. The Protocols even allow the Member States to adopt unlimited liability. In practice, only a limited number of countries adopted unlimited liability.\textsuperscript{404} The amounts set under the protocols are still nowhere near to the real possible costs of a major nuclear accident. Though there is no consensus on the estimation of the worst case scenario of nuclear accidents yet, the Chernobyl accident and Fukushima accident have caused damage much higher than the limit set in nuclear conventions. Some studies also estimate the possible damage to be as high as several billions of euros: it is estimated that the total damage of a reactor meltdown in Germany would be over 5,000 billion euro; a Greenpeace review of the costs cited some estimation varies from several billion to 6.8 trillion USD dollars.\textsuperscript{405}

Given the potential catastrophic losses the nuclear accidents can create, the limited liability creates a substantial subsidy to the nuclear industry. In theory, this subsidy might not only lead to less efficient care levels adopted by operators, but also place nuclear energy in an advantageous status compared to other kinds of energy. This may lead to a too high demand for nuclear energy as well. For example, a research showed that with a subsidy to nuclear sectors, the energy production cost for nuclear energy is lower than coal, gas and other renewable energy.\textsuperscript{406} A recent German research shows that if the total damage were born by the nuclear industry and all the liability is covered with insurance, it would lead to a net price increase for nuclear energy of 0.139 to 2.36 euro per kWh or 3.93 to 67.3 per kWh, depending

---

\textsuperscript{403} A different issue is of course whether there still could be liability under the national law of Member States which is, however, beyond the scope of this section. National Member State law was discussed \textit{supra} in Chapter 4.

\textsuperscript{404} For example, unlimited liability was adopted in Austria and Germany. In Denmark and Sweden, the unlimited liability is seriously considered or will be applicable when the revised Paris Convention comes into force. See Schwartz 2009, p. 54.

\textsuperscript{405} Cited in Currie 2008, p. 92.

\textsuperscript{406} Faure and Fiore 2009.
on the payout period. If this holds true, it will, undoubtedly, make the nuclear energy prohibitively expensive.

The international nuclear conventions also introduce a system of channelling the liability to nuclear operators. Other parties, such as suppliers, transporters, subcontractors, test operators, consultants, nuclear plant designers and constructors are released from liability. A right of recourse is only permitted if the nuclear incident is caused intentionally by others, or the contract explicitly so provides. This leads to the so-called legal channelling problem: other parties who actually contribute to the risks are relieved from liability and thus have no incentives to take efficient care. This problem has been criticized by much law and economics literature: after comparing the legal channelling under the international conventions and economic channelling in the US system, Vanden Borre argues that the legal channelling leads to underderterrence; Trebilcock and Winter criticize the combination of channelling and limited liability. The channelling is especially problematic since generally, it does not allow recourse. One could argue that the operators can negotiate with other parties and make arrangement to abolish channelling. However, this is not always possible for the nuclear industry. A survey shows that considering the different bargaining power, the contracts between operators and designers/constructors rarely make use of the exception to abolish channelling.

Finally, there is also criticism on the fact that public funds are used to compensate victims. Indeed, as explained above, under the Paris Convention, a three tiered compensation system is established. The Installation State needs to make public funds available to cover the second tier of damage and the contracting parties together should provide a collective fund to provide the third tier of compensation. The public funds intervention is even strengthened under the second generation of conventions. There was a shift towards public funding in those conventions. The required amount of public funds from Installation States under the Paris Convention is increased from (up to) 175 million SDRs to 500 million Euro, and the collective fund is increased from 125 million SDRs to 300 million Euro. The shift is also the case in the conventions under auspices of the IAEA. Under the original Vienna Convention, there is no requirement concerning public funds. The Protocol to the Vienna Convention adds a new tier - the public fund from the Installation State. A stand alone instrument, the CSC Convention, establishes a two-tier compensation system: 300 million SDRs from the Installation State or 300 million SDRs from the collective Fund. The shift towards public funding has been criticized by law and economic literature, since it constitutes a subsidy to operators and thus further dilutes the incentives for operators to take efficient care.

Hence, these criticisms formulated in the literature should be taken into account if one were to consider the model of the nuclear liability conventions as an example to be followed for a liability regime for the EU security industry. First of all one could question to what extent the nuclear industry in the 1960s is comparable to the security industry today and, second, the inefficiencies in the international nuclear liability conventions should also be taken into account when considering these conventions as a model to be followed in a potential liability regime for the EU security industry.

408 Vanden Borre 1999, p. 27.
410 Ameye 2010, p. 56.
411 Vanden Borre 2007, p. 305.
412 Faure and Vanden Borre 2008, 265-269.
5.3. Marine oil pollution

5.3.1. Brief summary of the regime

The international oil pollution compensation system consists of two important conventions that are somewhat interrelated. Two regimes are introduced briefly here: the first is composed of the International Convention on Civil Liability for Oil Pollution Damage (the CLC) and the second is the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (the Fund Convention). Those two conventions are important early conventions on oil pollution liability, and apply to ships carrying oil in bulk as cargo.

The international liability regime for oil pollution started to develop in the 1960s. The Torrey Canyon oil spill wakened the broad public awareness of the oil pollution risks. Before the coming into being of the international conventions, some voluntary scheme was adopted: the Tanker Owners Voluntary Agreement concerning Liability for Oil Pollution (the TOVALOP), under which fault liability with a reversal of the burden of proof is imposed on the tanker owner or the bareboat charter. The TOVALOP is complemented by another voluntary agreement by the oil industry: the Contract Regarding an Interim Supplement to Tanker Liability for Oil Pollution (the CRISTAL). The CRISTAL established a fund to cover oil pollution damage in addition to the TOVALOP with the contributions from oil industry.

Shortly after the adoption of the voluntary agreement, an international convention was reached under the auspices of the International Maritime Organization (IMO). In 1969, the 1969 CLC was passed, together with a Resolution on the Establishment of an International Compensation Fund for Oil Pollution Damage. This resulted in the adoption of the 1971 Fund Convention.

Two years after the adoption of the 1969 CLC, the 1971 Fund Convention was passed. The 1971 Fund Convention has two aims: to provide compensation when the protection available from the 1969 CLC is inadequate and to relieve the ship owners from additional financial burden.

5.3.2. Basis of liability

Strict liability is adopted in the 1969 Convention. Hot debates took place during the negotiation of the Convention on whom the liability should rest. Under the influence of the international regimes for nuclear liability, no doubts have been formulated on the reasonability of the channelling of liability. The debates focused on whether it should be the

---

413 This corresponds to Task 3.3 of Work Package 3 of the Invitation to Tender.
414 Although task 3.3 in the invitation to tender only refers to the International Convention on Civil Liability for Oil Pollution Damage we will also discuss the Fund Convention 1971 since this is strongly linked to the 1969 CLC Convention.
416 The original Fund Convention was adopted in 1971, and it was revised in 1992 (hereinafter the 1971 Fund Convention and the 1992 Fund Convention). The 1971 Fund Convention, 1110 UNTS 57, Cmnd 5061, the 1992 Fund Convention, RMC I.7.111, II.1.7.111, Misc 37 (1994), Cm 2658.
417 The 1992 CLC, Article I 11; the 1992 Fund Convention Article I 2.
419 The 1971 Fund Convention, Article 2(1).
ship owner or the oil industry that bears the liability. In the end, a compromise was made: liability under the CLC fell on the shoulders of the ship owner. As a price, the oil industry also needed to contribute to the compensation through a compensation fund. At the conference to pass the 1969 CLC, it was agreed that an international compensation fund would be established in the near future. Liability under the CLC is strict.

5.3.3. Liable persons

From what was just mentioned as far as the creation of the 1969 CLC and the 1971 Fund Convention is concerned it is clear that the 1969 CLC created a channelling of liability to the tanker owner. The ship owner is defined as “the person or persons registered as the owner of the ship or, in the absence of registration, the person or persons owning the ship.” The 1969 CLC pre-empts other legislations: no other claims are eligible other than those under the convention. It shows explicitly that no claims are made against the servants or agents of the owner. Scholars deduce from the explicit list that claims against other parties, for example, the cargo owner and the operator are still possible according to applicable national laws. Recourse against a third party is allowed under the 1969 CLC.

In 1992 two protocols were adopted to revise the original conventions. The 1992 CLC broadened the scope of persons that can be protected from the liability and this hence strengthens the effect of channelling.

According to the 1992 CLC, not only servants or agents of the owner, but also some other parties, such as the pilot or any other person who is not a member of the crew and performs services for the ship, any charterer, any person performing salvage with the consent of the owner or on the instructions of a competent public authority; any person taking preventive measures, and their agents or servants are also exonerated from oil pollution liability.

As we also mentioned with respect to the nuclear liability conventions the channelling of liability constitutes a major advantage for the security industry. To the extent that the security industry would (of course indirectly) be involved in marine oil pollution damage falling under the scope of the CLC (although it seems hard to imagine such a case) the security industry is protected by the channelling of liability: only the tanker owner can be held liable on the basis of the CLC, thus excluding liability of other parties including the security industry that may have contributed to the marine oil pollution.

5.3.4. Damage covered

This topic consists in fact of two separate issues. On the one hand there is the question of the amount of liability of the tanker owner; on the other hand the question arises what particular heads of damage will be compensated.

---

421 The 1969 CLC, Article I 3.
422 The 1969 CLC, Article III 4.
423 Verheij 2007, p. 141.
424 The 1969 CLC, Article III, 5.
425 See supra 5.2.3.
5.3.4.1. Limitation of liability

The liability established under the 1969 CLC was capped at 210 million francs or 2,000 francs for each ton of the ship’s tonnage. The amount is higher than that under the 1957 Convention on the Limitation of Ship-owners’ Liability, but still far from covering the whole potential damage that can be caused by oil pollution. The ship-owner’s right of limitation can not be used if the incident occurred as a resulted of his actual fault or privity.426

Several serious oil spills that happened after the adoption of the original CLC and the Fund Convention - for example, the Amoco Cadiz in 1978 and the Tanio in 1980 triggered the revisions to the original conventions. The first Protocols to revise the conventions were reached in 1984. Since the US did not ratify the protocols, the protocols could not come into force. Nevertheless, the changes in the 1984 protocols are largely incorporated in the 1992 Protocols.

In 1992, two protocols were adopted to revise the original conventions: the 1992 CLC and the 1992 Fund Convention. This 1992 CLC increased the limit of liability to 4.51 million SDRs or 89.77 million SDRs, depending on the size of the ships. As a compromise to the increase of the liability limit, the criteria when the ship owners lose their right to limit liability are further constricted: damage should result from their wilful misconduct.427

5.3.4.2. Damage covered

According to the 1969 CLC, the convention applies to pollution damage that happened on the territory (including territorial sea) of a Contracting Party and applies to the preventive measures.428 Oil pollution is defined as:

Loss or damage caused outside the ship carrying oil by contamination resulting from the escape or discharge of oil from the ship, wherever such escape or discharge may occur, and includes the costs of preventive measures and further loss or damage caused by the preventive measures.429

This definition is constricted by the word “contamination”, which means that damage caused by fire or explosion following a discharge is not covered. The definition is still vague and its concrete scope only became clear over years. Personal injury is eligible for compensation, but not including exposure to health risks, anxiety and upset. Damage to property should be “real” and not speculative. Pure economic loss is eligible if the loss is quantifiable in economic terms.430 A more problematic category is damage to the environment. Preventive measures contain clean-up and restoration. They are compensable if they are reasonable and the loss is quantifiable in economic terms. The claims based on abstract methods calculation are not admissible.431

However, the 1992 CLC has broadened the definition of pollution damage. It now includes:

426 The 1969 CLC, Article V 2.
427 The 1992 CLC, Article V, 1.2.
428 The 1969 CLC, Article II.
429 The 1969 CLC, Article I, 6.
430 Verheij 2007, p. 138-139.
431 Id, p. 139.
(a) loss or damage caused outside the ship by contamination resulting from the escape or discharge of oil from the ship, wherever such escape or discharge may occur, provided that compensation for impairment of the environment other than loss of profit from such impairment shall be limited to costs of reasonable measures of reinstatement actually undertaken or to be undertaken;
(b) the costs of preventive measures and further loss or damage caused by preventive measures.\footnote{432}

This definition further delimitates the scope of compensable environmental damage. The loss of profit from the impairment of the environment is compensable, including both consequential loss and pure economic loss. In addition to that, the term “impairment of the environment” is limited to the costs of reasonable measures of reinstatement actually taken or to be undertaken. Even with this definition, its clear implication has to be understood in practice. Disputes have taken place on the issues of damage quantification, the state as environmental trustee and ecological restoration.\footnote{433} It is often up to the national courts, where the lawsuits are brought, to interpret the meaning of vague terms such as “reasonable measures”.

5.3.5. Exclusions and defences

As far as the marine pollution liability conventions is concerned one should make a distinction between on the one hand exclusions that could exclude the strict liability of the tanker owner and on the other hand exclusions that would lead the ship owner to loose his right of limitation. In the latter case the exclusion would hence not be a defence, but to the contrary, a reason to enlarge the scope of liability of the tanker owner.

Liability is excluded according to Article III of the CLC if the owner proves that the damage:

(a) resulted from an act of war, hostilities, civil war, insurrection or a natural phenomenon of an exceptional, inevitable and irresistible character, or
(b) was wholly caused by an act or omission done with intend to cause damage by a third party, or
(c) was wholly caused by the negligence or other wrongful act of any government or other authority responsible for the maintenance of lights or other navigational aids in the exercise of that function.

Article III(3) moreover holds that if the owner proves that the pollution damage resulted wholly or partially either from an act or omission done with intend to cause damage by the person who suffered the damage or from the negligence of that person, the owner may be exonerated wholly or partially from his liability to such person.

As far as the limitation of liability is concerned Article V(2) of the CLC provides that the owner shall not be entitled to limit his liability under the convention if it is proved that the pollution damage resulted from his personal act or omission, committed with the intent to cause such damage, or recklessly and without knowledge that such damage would probably result.

\footnote{432}{The 1992 CLC, Article I 6.}
\footnote{433}{Mason 2003, p. 3-5.}
5.3.6. Causation

Like it was mentioned for the nuclear liability conventions (see supra 5.2.6) there is no specific article dealing with causal uncertainty or, more generally, with the question of how causation should be proven in the CLC. However, there is, like in the nuclear case, an arrangement for the case that multiple tortfeasors would be involved in the marine pollution incident. Article IV of the CLC provides that when an incident involving two or more ships occurs and pollution damage results there from, the owners of all the ships concerned, unless they are exonerated as explained above,\textsuperscript{434} shall be jointly and severally liable for all such damage which is not reasonably separable. Again, a rule is followed of joint and several liability unless a reasonable separation of the damage would be possible.

5.3.7. Relation with regulation

Again a parallel with the nuclear liability case applies in the sense that the liability imposed upon the ship owner according to the CLC is considered as a strict liability. Hence, breach of a regulation is not required for the ship owner to be held liable under the CLC. The opposite is also the case: compliance with regulatory standard will not free the ship owner from liability if the conditions for such liability under the CLC apply.

5.3.8. Financial security and compensation mechanism

Again a distinction should be made on the one hand between the mandatory financial security imposed via the CLC and on the other hand additional funding which is provided via the Fund Convention.

5.3.8.1. Financial security

The 1969 CLC requires the owner of a ship registered in a contracting state and carrying more than 2,000 tons of oil in bulk as cargo to maintain insurance or other financial security up to his limits of liability. In addition to insurance, the financial security can also be in form of bank guarantee or a certificate delivered by an international compensation fund.\textsuperscript{435} This requirement remains in the 1992 CLC.\textsuperscript{436} Similar provisions can also be found in the Bunker Convention.\textsuperscript{437} Though both regimes allow insurance and other instruments to be used to cover the liability, the most popularly used instruments are insurance, especially Protection and Indemnity Policies (P&I Policies).

5.3.8.2. Additional funding

In addition to the financial security provided to back up the (limited) liability of the tanker owner additional funds are provided via the Fund Convention. This Fund Convention has, however, gone through various evolutions that have to be sketched now.

The 1971 Fund Convention plays two roles: to compensate the victims and to indemnify the ship owners. Firstly, it complements the compensation from the 1969 CLC under these

\textsuperscript{434} See above 5.3.5.
\textsuperscript{435} The 1969 CLC, Article VII 1.
\textsuperscript{436} The 1992 CLC, Article VII.
\textsuperscript{437} The Bunker Convention, Article VII.
situations if: no liability can be established under the 1969 CLC and if; owners and their financial guarantors are financially incapable of compensation and the damage exceeds the owners' liability. To encourage preventive measures, the costs raised from the voluntary activities of the owners are also treated as pollution damage.\footnote{The 1971 Fund Convention, Article 4(1).} The Fund has no obligation to pay if it can prove that the damage resulted from an act of war, hostilities, civil war or insurrection or oil from a warship or a state owned/operated ship; or if the claimant cannot prove that damage resulted from a ship-related incident. Contributory negligence can also be used as a defence for the fund.\footnote{The 1971 Fund Convention, Article 4(2)(3).}

The compensation available from the 1971 Fund is not unlimited: the total sum of the amount from the 1969 CLC and the 1971 Fund Convention is capped at 450 million francs; for the damage caused from a natural disaster of an exceptional, inevitable and irresistible character, the amount payable from the Fund is capped at 450 million francs. The Assembly of the Fund has the right to increase the amount up to 900 million francs. When claims exceed the amount payable from the fund, payment should be reduced proportionally for each claimant.\footnote{The 1971 Fund Convention, Article 4(4)(5)(6).}

In addition to providing complementary compensation to victims, the 1971 Fund also indemnifies the ship owners. Indemnification is available for the payment between (1) the amount in excess of 1, 500 francs for each ton of the ship’s tonnage or 125 million francs, whichever is less; and (2) the amount not in excess of 2,000 francs for each ton of the said tonnage or 210 million francs, whichever is less. But the indemnification is not available if the damage is caused from the wilful misconduct of the ship owners.\footnote{The 1971 Fund Convention, Article 5(1).} Claims to compensation or indemnification should be made within three years from the occurrence of the damage and six years from the occurrence of the incident.\footnote{The 1971 Fund Convention, Article 6(1).}

The Fund is financed by big oil importers in contracting states. The eligible importers need to make initial contributions as the working capital of the fund, and the annual contributions to cover the administrative expenses and claims.\footnote{Chao 1996, p. 98.} The calculation of contributions is based on a fixed sum for each ton of contributing oil received.\footnote{The 1971 Fund Convention, Articles 11(1), 12(2).} The Contracting State has the obligation to ensure that the eligible contributing importers appear on a list and to communicate it to the Fund.\footnote{The 1971 Fund Convention, Article 15(1).} The Contracting State can also declare that it assumes the obligation that lies on the importers within its territory to make contributions.\footnote{The 1971 Fund Convention, Article 14(1).}

5.3.8.2.1 The 1992 Fund and the winding up of the 1971 Fund

The original CLC and Fund Convention proved to be insufficient to cover the potential catastrophic oil pollution damage. In 1992 a new compensation fund was established. The 1992 Fund Convention removed the function of the Fund to alleviate the burden of liability of ship owners. Therefore the only function of the 1992 Fund is to provide additional protection to the victims of oil pollution. The conditions of the application of the 1992 Fund to
compensate victims are the same as that of 1971 Fund. The available compensation from the 1992 CLC and the 1992 Fund Convention is increased to 203 million SDRs.

The 1992 Fund is also financed by the oil industry. To remove an obstacle for ratification, the requirement of the considerable initial contributions is removed. The 1992 Fund is solely financed by annual contributions. The calculation of the contributions is also based on the amount of oil received.

The 1992 Fund Convention came into force in 1996, when the 1971 Fund Convention was still in force. The co-existence of the two funds was problematic since that diluted the capacity of each fund to provide sufficient compensation. In 2000, a protocol was passed to allow for an early winding up of the 1971 Fund. According to this protocol, the 1971 Fund ceases to be in force when the number of contracting states falls below twenty-five, or the total quantity of contributing oil fell below 100 million tons, whichever is earlier. The 1971 Fund ceased to be in force on 24 May 2002. But it still continues in compensating for damage from incidents before that day. As of January 2012, the 1992 Fund Convention has 105 Member States.

5.3.8.2.2 The 2003 Supplementary Fund

Although the limitation of compensation under the 1992 Fund Convention had been considerably increased, shortly after its adoption, the amount was dwarfed again by yet other catastrophic oil pollution cases. Under this background, a Supplementary Fund was established in a 2003 Protocol. The Supplementary Fund provides an additional layer of compensation for oil pollution victims under the 1992 CLC and the 1992 Fund Convention. In other words, a condition for the payment from the Supplementary Fund is that the victim is entitled to compensation under the 1992 CLC and the 1992 Fund Convention, and is unable to obtain full and adequate compensation from them. The Supplementary Fund Convention increases the aggregated amount of compensation up to 750 million SDRs.

5.3.9. Rules of evidence

Also on this issue there are no particular rules in the CLC. Since no specific rules apply it is in principle up to the injured party, the plaintiff, to prove that the conditions for liability are fulfilled. The CLC is only clear in Articles III(2) and (3) that if the owner wants to call on a ground of exclusion of liability it is the owner that must prove that the reasons for such an exclusion of liability are fulfilled. The CLC does not have any particular rules with respect to a reversal of the burden of proof.

---

447 The 1992 Fund Convention, Article IV 1.
448 The 1992 Fund Convention, Article IV 4.
450 The Nakhtodka accident near Japan in 1997 and the Erika disaster in France in 1999 are two examples.
452 The Supplementary Fund Convention, Article IV 1.
453 The Supplementary Fund Convention, Article IV 2.
454 Referred to under 5.3.5 above.
5.3.10. Jurisdictional and procedural issues

There are several procedural issues mentioned in the CLC which are worth mentioning. A first point is that Article II clearly provides that the Convention exclusively applies to pollution damage caused

- in the territory, including the territorial sea of a contracting state, and
- in the exclusive economic zone of a contracting state, established in accordance with international law or otherwise in a zone not extending more than 200 nautical miles.

Pollution damage that falls outside of this territory and would e.g. be caused in high seas would hence not fall within the scope of the CLC.

According to Article IX of the Convention, where an accident has caused pollution damage in the territory, including the territorial sea or exclusive economic zone of one or more contracting states or preventive measures have been taken to prevent or minimize pollution damage in such territory actions for compensation may only be brought in the courts of any such contracting state or states. Reasonable notice of any such action shall be given to the defendant and each contracting state shall ensure that its courts possess the necessary jurisdiction to entertain such actions for compensation. Moreover, Article X provides that any judgment given by a court with jurisdiction in accordance with Article IX which is enforceable in the state of origin where it is no longer subject to ordinary forms or review shall be recognized in any contracting state except:

- where the judgment was obtained by fraud;
- where the defendant was not given reasonable notice and faire opportunity to present his case.

Article VIII moreover provides that the rights of compensation under the CLC shall be extinguished unless an action is brought within three years from the date when the damage occurred. However, in no case shall an action be brought after six years from the date of the incident which caused the damage. Where the incident consists of a series of occurrences the six years period shall run from the date of the first occurrence.

5.3.11. Conclusions Marine Oil Pollution and relevance to the security industry

The relevance for the security industry was already briefly alluded to. It may be rare that the security industry would be involved in marine pollution incidents coming under the scope of the CLC. But in the event that this were the case the major advantage for the security industry would be that the liability is exclusively channelled to the tanker owner, thus excluding the possibility of holding the security industry liable according to the CLC.

If the question is asked to what extent the CLC and Fund Convention could constitute an interesting model for a potential future liability regime for the EU security industry we should again refer to what was also mentioned when discussing the nuclear liability conventions: the marine pollution liability conventions present a few interesting features, but not necessarily features that should be followed in another liability regime for the simple reason that one has to consider those features within a particular historical context. For example the financial cap (limit) on the liability of the ship owner has to be considered in the light of the fact that the

---

455 Article IX(2) of the CLC.
The drafters of the 1969 CLC were already aware of the fact that later (in 1971) a Fund Convention would be drafted. Hence, the financial limit on the liability of the tanker owner would be compensated with a supplementary compensation mechanism (the 1971 Fund) financed by the oil industry.

The limitation on liability has substantially increased since 1969, but is criticised. The literature has considered this limitation as an “historical mistake”. After all, the problem with a financial limit on liability is that the ship owner is not fully exposed to the social costs of his activity. The international liability regime shows also other inefficiencies. One such inefficiency, criticised in legal doctrine is precisely the channelling of the liability to the ship owner. The channelling of liability to ship owners can also be explained from the private interest approach. During the negotiation of the CLC, various proposals have been made by delegates from different states. For example, Ireland, the Netherlands and Denmark advocated strict liability on the cargo; US, UK, Australia and Germany were in favour of strict liability on ship; other proposals included fault liability on the ship owner and joint liability. Those debates are understandable, the countries with a big ship industry preferred liability on cargo; while on the other hand, countries with a powerful oil industry proposed liability on ships.

Also the financial cap on liability has been criticised in the literature. An early empirical study has shown that by increasing the amount of compensation from $52 million (the limit of that moment) to $250 million, the effect on the price of oil is quite limited. Even when some small oil companies are driven out of business due to unlimited liability, it is not necessarily undesirable since only when facing the whole liability they create, they will take optimal care.

There is, however, one important difference between the additional funding provided in the international nuclear liability regime on the one hand and in the marine oil pollution regime, discussed here on the other hand. Under the international nuclear liability conventions the additional funding was entirely provided through public funding and hence constitutes a subsidy to the nuclear industry. The 1979 and 1992 funds are not at all financed through public funding, but through the oil industry. There is hence no subsidy. Of course, one may question the efficiency of the fund since it is the oil industry, rather than the liable party – ship owners who finance the compensation. However, this needs to be understood against the background of the balance of interests between ship owners and oil industry. However, the efficiency of such funds can still be questionable, since the contributions of the funds are based on the amount of oil received. Therefore, the oil importers still lack incentives to choose safer ships.

5.4. Other relevant treaties

In this section, the following treaties are discussed: the 2010 International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea (5.4.1), the 2003 Protocol on Civil Liability and Compensation for Damage Caused by the Transboundary Effects of Industrial Accidents on Transboundary Waters (5.4.2) and the 1971 United Nations Convention on International Liability for Damage Caused by Space Objects (5.4.3).

---

459 Smets 1983, p. 31-43.
461 This has been criticized as soon as the 1971 Fund Convention is adopted. See Wood 1975, p. 46-47.
5.4.1. The International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, 2010 (2010 HNS Convention)\footnote{The International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea (HNS Convention) has been adopted on 3 May 1996 but did not enter into force until 2010; that entry into force was in fact superseded by the 2010 Protocol which was adopted on 30 April 2010; but which has not entered into force.}

5.4.1.1. Brief summary of the regime

The carriage of hazardous and noxious substances\footnote{According to Article 1 of the HNS Convention these substances are: oil, noxious liquid substance, defined in regulation 1.10 of Annex II to the International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto, as amended, and those substances and mixtures provisionally categorized as falling in pollution category X, Y or Z in accordance with regulation 6.3 of the said Annex II; dangerous liquid substances carried in bulk listed in chapter 17 of the International Code for the Construction and Equipment of Ships Carrying Dangerous Chemicals in Bulk, as amended, and the dangerous products for which the preliminary suitable conditions for the carriage have been prescribed by the Administration and port administrations involved in accordance with paragraph 1.1.6 of the Code; (iv) dangerous, hazardous and harmful substances, materials and articles in packaged form covered by the International Maritime Dangerous Goods Code, as amended; liquefied gases; liquid substances carried in bulk with a flashpoint not exceeding 60°C; solid bulk materials possessing chemical hazards covered by the International Maritime Solid Bulk Cargoes Code.} might lead to accidents and endanger human health as well as environmental and economic interests. The International Convention on Civil Liability for Oil Pollution Damage (hereafter CLC) has established a liability regime which governs compensation for oil pollution damage.\footnote{As has been discussed in detail in section 5.3 supra.} Nevertheless, there is a large bulk of accidents which resulted from the carriage of hazardous substances other than the substance which is governed by the CLC Convention, being oil. The International Convention on Liability and Compensation for Damage in connection with the Carriage of Hazardous and Noxious Substances by Sea (hereafter the HNS Convention) has been concluded for addressing liability and compensation issues concerning damage resulting from the carriage of such substances.

Personal injuries, environmental damage, economic losses and the costs of preventive measures which resulted from the carriage of hazardous and noxious substance by vessels are governed by the HNS Convention.\footnote{Article 1 of the HNS Convention.} The type of damage which is governed by the HNS Convention varies concerning the place of accident. According to Article 3, the scope of application of this convention is divided into 4 sections: (1) in the territory of a State Party, all the damage is governed by the Convention, (2) in the exclusive economic zone of a State Party, only environmental damage is governed by the HNS Convention, (3) on board a ship registered in a State Party or, in the case of an unregistered ship, on board a ship entitled to fly the flag of a State Party all the damage is governed by the HNS Convention other than environmental damage which has been caused by the HNS carried by the ship, and (4) preventive measures are governed by the Convention everywhere they have been taken.

Furthermore, the scope of the Convention has been excluded from damage subject to the jurisdiction of the CLC Convention, damage resulting from radioactive material, warships, any kind of Government non-commercial service, the contractual claims and workers’ compensation or social security schemes.\footnote{Article 4 of the HNS Convention.} The HNS Convention, due to the type of substances which are categorized as hazardous substance, primarily imposes a strict liability regime on the owner of the ship. On the other hand, the owner is required to maintain
compulsory insurance or similar financial security up to the limitation of liability. In addition, the owner will enjoy the limitation of liability to the certain amounts articulated in the HNS Convention, only if the owner complied with the conditions of the HNS Convention.\textsuperscript{467}

On the other hand, the HNS Fund has been established for supporting a limitation of liability of the owner. If the amount of damage exceeds the financial cap or no liability for the damage arises under the liability of the owner or even if owner is financially incapable to compensate the victims, the HNS Fund will pay compensation under specific regulations which are articulated in the Convention.\textsuperscript{468} The HNS Fund has both a general account for all types of substances and a separate account for specific substances such as oil, Liquefied natural gas (LNG) and liquefied petroleum gases (LPG). The HNS Fund has been supported by initial and annual contributions of the “receiver” in the State party. For each type of substance, that has a separate account or a general account, specific total quantities of imported substances have been specified by the Convention. In case the total quantities of the substance exceed the amounts which are clarified in the convention, the receiver shall pay a contribution.\textsuperscript{469} The amount of the contributions and other related regulations are determined by the HNS Fund on a yearly basis.

5.4.1.2. Basis of liability

The nature of the carriage of substances under the application of the HNS Convention is dangerous and has a high probability of accidents. Therefore, according to tort law he who carries on a dangerous activity is liable for the harm imposed by the activity. The liability regime in the HNS Convention is based on strict liability. According to article 7 of the HNS Convention, the owner of the ship is liable for the damage which results from any hazardous or noxious substance during the carriage by ship. The owner of the ship is the most appropriate person who can prevent the damage. In particular if the owner has been held liable based on strict liability, the owner will carry on measures for prevention of the damage. However, there are exceptions to the strict liability regime, more particularly if the damage resulted from force majeure such as war, insurrection, or an inevitable natural disaster, the owner will not be liable under the HNS Convention.\textsuperscript{470}

Although the nature of the carriage of the HNS substance has mostly required input from the ship owner for the prevention of accidents, some other factors might also be involved in the accident risk, which are not controlled by the owner. As Shavell states, accidents sometimes have a bilateral dimension.\textsuperscript{471} In other words, in some cases the behaviour of the victims or the third parties plays an important role in the risk. This has been noticed in the HNS Convention. According to Article 7, if the damage caused by the negligence or omission of any respective government, other responsible persons for providing navigational aids, the shipper or any other responsible person does not prove adequate information concerning the hazardous and noxious nature of substances, the owner will not be held liable. In addition, if the damage caused by the intentional act or omission of a third party, the owner will be excluded from liability. Other involved persons such as the ship crew and even the persons who are taking preventive measures will not be held liable, unless the damage resulted from their act or omission with the intent of damage or reckless act with knowledge about the possible risks.\textsuperscript{472}

\begin{flushright}
\textsuperscript{467} Article 9 of the HNS Convention.
\textsuperscript{468} Chapter 3 of the HNS Convention.
\textsuperscript{469} Articles 16, 17, 18 and 19 of the HNS Convention.
\textsuperscript{470} Article 7 of the HNS Convention.
\textsuperscript{471} Shavell 2007, p. 139.
\textsuperscript{472} Ibíd.
\end{flushright}
5.4.1.3. **Liable persons**

Ship accidents might have various reasons, including internal causes and external causes. Nonetheless, since most of the ship accidents are caused by human errors, the owner of the ship has will be held prima facie liable. The causes of the accident can be related to a defect in the ship or cargo or to environmental conditions. The owner of the ship according to article 1 is defined as the person or persons registered as the owner of the ship or the person or persons owning the ship. However, in the case of a ship owned by a State and operated by a company which in that State is registered as the ship's operator, "owner" shall mean such company. Thus, the registered owner or the actual owner of the ship is presumed one who has most incentive for prevention from accidents by establishing a strict liability rule.

However, the owner of the ship might be excluded from liability, if the owner can prove that the accident was caused by other persons or by force majeure such acts as war, hostilities, civil war and insurrection or a natural phenomenon with exceptional, inevitable and irresistible conditions. Moreover, if it has been proved that the damage wholly caused by the act or omission of a third party, the owner would not be held liable. Although, it seems that if the damage partly caused by a third party, the owner would not enjoy an exclusion of liability. A similar condition is articulated for the damage resulting in a wrongful act of authorities responsible for the maintenance of navigational aids including governments. Since, the nature of the substance which is carried by the ship has a great impact on the occurrence and prevention of accidents, information about the type of substances plays an important role for prevention and minimizing of accidents.

Yet, if the shipper or any other person who is responsible for providing information concerning the hazardous nature of substances fails to fulfil this act, the owner would not be held liable for the damage. In cases that the owner and his servants reasonably know the hazardous nature of substance, they will be held liable, but if typically they don't know or ought not to know the risks of such substance, it is the responsibility of the shipper or other respective person to inform them. However, the methods for notifying such information or details about the extent of the hazardousness of those substances not clarified in the HNS Convention.

All other involved people in the accident and prevention measures, including members of the crew, agents or servants of the owner, or salvage persons will not be held liable unless the damage resulted from their act or omission intentionally or recklessly. If two or more ships which are carrying noxious or hazardous substances are involved in an accident, each of the ship owners will be held separately liable for full compensation. However, a joint liability regime will be applied in the mentioned case if damage would not be separable. In cases that damage resulting from an HNS ship is not separable from other factors, all the damage is deemed to result from the NHS ship. This is only different if that other damage would be subject to the convention on civil liability for oil pollution damage 1969 or would be radioactive material damage according to international maritime dangerous code.

In addition to the right of recourse for the owner which has been noticed several times in the Convention, channelling of liability to the ship owner in case of causal uncertainty, where

---

475 Article 7 of the HNS Convention
476 Article 8 of the HNS Convention.
477 Ibid.
478 Articles 1 and 4 of the HNS Convention.
479 Articles 7, 8 and 19 of the HNS Convention.
multiple parties may have contributed to the risk, would not expand the scope of liability and consequently the insurability. Whereas the liability of the owner is limited by the financial cap in the Convention, the channelling of liability to the ship owner in case of uncertainty would not lead to insurability of damage. It is noteworthy to mention that all the damage which falls under the scope of the HNS Convention and exceeds beyond the owner liability limit or in cases that no liability arises for the owner, will be paid by the NHS Fund.\footnote{Chapter III, Articles 13 and 14 of the HNS Convention.} Thereupon, the cost of uncertainty is shared between the stakeholders in the NHS Fund.

5.4.1.4. Limitation of liability

There are two arrangements for the limitation of liability under the HNS Convention. A first tier is allocated to the liability of the ship-owner and a second tier is dedicated to the compensation duty of the HNS Fund. The ship owner may limit his liability depending on the tonnage of the ship and the form of substances which were transported to the certain financial amount under the HNS Convention. If the amount of the damage exceeds the limited liability of the owner, the NHS Fund pays the exceeded compensation amount. Limitation of the liability regime under the NHS Convention is divided into twofold, based on the kind of substances which are carried by the ship. Those two forms are categorized by the HNS Convention as the bulk form and the packaged form.\footnote{Article 1 of the HNS Convention.} However, the main criterion for the limitation of liability is based on the tonnage of the ship either for the bulk or packaged forms. In this regime, the tonnage of the ship for each of the form is considered as baseline and accordingly a certain amount of units is presumed as compensation amount. The rate of calculation of the compensation is diminished up to increasing of tonnage of the ship.

For damage that has been caused by a bulk ship, up to 2,000 tonnage ship, 10 million units of account shall be paid by the owner. When the ship’s tonnage exceeds this tonnage, the following amount shall in addition be paid by the owner. For each unit of tonnage from 2,001 to 50,000 units of tonnage, 1,500 units of account; for each unit of tonnage in excess of 50,000 units of tonnage, 360 units of account.\footnote{Article 9 of the HNS Convention.} Furthermore, the total aggregate amount of compensation for each accident is 100 million units. For packaged HNS a similar baseline of tonnage of the ship has been set up by the HNS Convention. Nevertheless the amount of compensation in case of a packaged ship is higher than in case of a bulk ship and the total aggregate amount for a packaged ship is 115 million per case.\footnote{According to Article 9 of the convention, where the damage has been caused by packaged HNS, 11.5 million units of account for a ship not exceeding 2,000 units of tonnage; and for a ship with a tonnage in excess thereof, the following amount in addition to that mentioned in: for each unit of tonnage from 2,001 to 50,000 units of tonnage, 1,725 units of account; for each unit of tonnage in excess of 50,000 units of tonnage, 414 units of account.} Whenever the damage has been caused by both bulk HNS and packaged HNS, or where it is not possible to determine whether the damage originating from that ship has been caused by bulk HNS or by packaged HNS, the packaged form regulation will be applied.

The establishment of the limitation of liability allows the insurability of such damage and consequently a better compensation of victims. One may argue that limitation of liability might decline the incentive of the owner for prevention from the accidents combined with the compulsory insurance clause of the HNS Convention.\footnote{Article 12 of the HNS Convention.} For prevention of such misfeasance, if the damage resulted from the personal act or omission of the owner intentionally or recklessly, the owner is not entitled to enjoy the limitation of liability subject to HNS
Convention. Nevertheless, in the absence of regulation which requires due care behaviour from the owner, a moral hazard risk might emerge, since the aforementioned article only encompass intentionally or recklessly committed act or omissions of the owner.

Furthermore, the owner shall establish a fund under Article 9 of the HNS Convention in order to benefit from the limitation of liability. This fund shall be constituted by a deposited total amount of compensation (based on the tonnage and form of carriage) or providing a financial guarantee acceptable under the regulation of the state party where the fund is constituted. After constitution of the fund all the claims shall be brought before the fund and none of the assets of the owner, other than the fund, shall be arrested.

The second tier of compensation is assigned to the HNS Fund. The HNS Fund has been established for compensating damage under the HNS Convention for three purposes: primarily when the total admissible claims exceed the ship owner’s liability; secondly, when the owner or the insurer are not financially capable to cover the claims for compensation for damage in the first tier; and thirdly when the owner has not been held liable under the HNS Convention. Nonetheless, the Fund will not pay any compensation, if the damage was caused by an act of war, etc., or by HNS discharged from a Government owned non-commercial ships, or if the claimants cannot prove the causal link between damage and an incident involving HNS ships. Therefore the Fund reasonably covers the HNS damage other than the damage caused by the hostilities and government owned non-commercial ships. In addition, similar to the liability of the owner, the damage resulted from an act or omission done intentionally to cause damage by the person who suffered the damage or from the negligence of that person will not be compensated by the Fund.

The duty to compensate the HNS Fund is also limited by a financial limit. For this propose, if the aggregate amount of the damage exceeds the ship owner’s liability, the compensation will be paid up to 250 million units for any specific accident. In some cases, where no liability is attached to the ship owner, the aggregate amount of compensation will be 250 million units of account. Thus, the utmost aggregate amount which might be paid under the HNS Convention for damage will be 250 million units. In case the amount of damage is much higher than the payable compensation by the Fund, the amount of payment will be divided between claimants with an equal proportion of their admissible claims, other than in respect of death or personal injury which has priority over other claims up to two-thirds of the total amount. Moreover, compensation in accordance with this HNS Convention might be paid, even if the owner has not constituted a fund by the HNS Fund assembly.

In sum it might be held that the liability under the HNS Convention has been limited to two levels: the first tier for the ship owner’s liability and in the second tier for the HNS Fund. Nevertheless, since the amount of compensation due by the Fund also has a limit, if the amount of damage exceeds the limit, the damage can only be compensated up to the limited amount. Therefore, there is still a possibility that damage which falls under the HNS Convention is partially not compensated.

---

485 Article 9 of the HNS Convention.
486 Article 10 of the HNS Convention.
487 Article 14 of the HNS Convention.
488 According to Article 14, if the HNS Fund proves that such damage resulted from an intently act of the victim, it may be exonerated from its obligation to pay compensation to such person although not for preventive measures.
489 Article 14(5) of the HNS Convention.
490 Article 14(7) of the HNS Convention.
5.4.1.5. Relationship with regulation

For analyzing the regulations under the HNS Convention, the ex-ante (before the accident) and ex-post (after the accident) regulations should be considered separately. Although the ex-ante regulation has not been taken into account directly, ex-post regulation has to some extent been considered in the HNS Convention. The ex-ante regulations such as licenses and standards are not directly subject to HNS Convention. Compliance with regulation is of importance for the receiver, ship owner and insurer. The receiver shall pay a contribution based on the aggregate amount of the cargo which is received in one calendar year as contribution to the HNS Fund as required to make payments for damages. The amount of the contribution is determined by the Fund Assembly based on the total amount of cargo, income and expenditure of the HNS Fund. The main expenditure of the Fund is the cost for compensation which shall be paid after the accident. Thus, there is direct link between the amount of contribution and the compensation which is paid by HNS Fund. If the number and cost of damage has increased the amount of contribution would increase consequently. Therefore, the receiver has an approximate incentive to articulate some contractual conditions over the carriage of cargo for prevention of accidents.

According to Article 12 of the HNS Convention, the owner enjoys a limitation of liability if the owner maintains insurance or other types of financial guarantee. In case of insurance, the risk shifts from the owner to the insurer based on the insurance certificate. In Article 12 of the HNS Convention, it has also been envisaged that the respective state authority shall issue the insurance certificate. The insurance company which has made insurance contract might establish some contractual requirements for prevention in case of accidents and consequently control the behaviour of the owner. In addition to the contractual provision, the insurer can also rely on regulations for the prevention accidents. Therefore, ex-ante regulations, although they have not been mentioned directly in the text of the HNS Convention, based on the contractual provisions in the insurance policy they might still play a role.

In the HNS Convention, the preventive measure has been defined as “any reasonable measures taken by any person after an incident has occurred to prevent or minimize damage.” Thus, the preventive measure in the HNS Convention means: the measure which prevents the extension of the damage not the occurrence of the accident. Any specific regulation such as following a code of conduct has not been prescribed in the HNS Convention for regulating the behaviour of the owner or other involved persons. Nevertheless, the owner has an incentive for implementing the preventive measures for minimizing the damage. The costs of preventive measures have been defined as damage and are accordingly compensable both under the liability of the ship-owner and by the HNS Fund. Wherever preventive measures take place, they are included in the scope of the HNS Convention. Although the HNS Fund might be exonerated in some particular circumstance from the obligation to pay compensation, this exoneration shall not apply to preventive measures. Moreover, according to Article 15, the Fund can allocate some credit facilities based on its internal regulations for implementation of preventive measures against such damage which might be compensated by the fund under the HNS Convention.

491 Articles 18, 19 and 20 of the HNS Convention.
492 Article 15 of the HNS Convention.
493 Article 17 of the HNS Convention.
494 Article 1 of the HNS Convention.
495 Articles 1 and 14 of the HNS Convention.
496 Article 3 of the HNS Convention.
497 Article 14 of the HNS Convention.
Thus, there is no obstacle for performing such measures for minimizing the damage by the owner or other persons under the regulation of the HNS Convention. Nonetheless, there is not any specific regulatory framework under the HNS Convention for this end. In that respect, it might be discussed whether compliance with a regulation would lead to an exclusion of liability or vice versa, whether a breach of regulation would lead to liability. However, there is no direct relationship between liability and regulation which affects the scope of the liability regime.

5.4.1.6. Causation

The requirement of proving a causal link will have an important impact on determination of liability. Different methods might be applied for re-establishing the causal link. According to the HNS Convention, the main criterion is the damage which is occurring during carriage of hazardous or noxious substances by ship. The type of causes i.e. fire or explosion is not cleared and it seems that all the damage which directly or indirectly resulted from those substances could fall under the provisions of the HNS Convention.\(^{498}\) Thus, the only causal link which should be proved is that the damage resulted from those listed hazardous and noxious substances and that they were carried by ship. Even though, in cases that the HNS damage was mixed with other factors, it may not be possible to separate the damage which resulted from those substances from other damage which resulted from the other factors. In that case all damage shall be deemed to have resulted from the hazardous and noxious substances, except such damage which is expressly excluded from the scope of the HNS Convention.\(^{499}\)

Furthermore, in case of a series of accidents, if they have the same origin, the liability shall attach to the owner at the time of the first of such occurrences. Thus, in case of carriage of hazardous and noxious substances by ship, even if other factors were involved as well, the owner will be held liable. However, no specific criterion has been provided for establishing a causation between the damage and hazardous substances in the HNS Convention. A problem, in the particular in case of environmental damage might emerge when there is uncertainty concerning the extent of such damage. The burden of proof of causation between the damage and hazardous substances under the HNS Convention rests on the plaintiff. There might be damage which resulted from an NHS ship, but not as a result of the carriage of hazardous and noxious substance. Even if it was proved that other factors were also involved in the occurrence of the damage, the liability is still strictly channelled to the owner. Thus, in case of uncertainty concerning the environmental damage caused by some types of hazardous substances, the establishment of causation will be difficult for the plaintiff. The rules on causation are subject to the jurisdiction of the local court.\(^{500}\)

5.4.1.7. Damages

The HNS Convention encompasses various types of damage which might result from carriage of hazardous and noxious substances by ship. However, different rules might be applied to different types of damage based on the place of the accident. Damage includes personal injury, property damage, contamination of the environment, economic losses, the costs of

\(^{498}\)Article 1 of the HNS Convention.

\(^{499}\)According to Article 4 pollution damage as defined by CLC Convention, damage caused by a radioactive material of class 7 either in the International Maritime Dangerous Goods Code, damage caused by the warships, naval auxiliary or other ships owned or operated by a State and used, for the time being, only on Government non-commercial service.

\(^{500}\)Articles 9 and 10 of the HNS Convention.
preventive measures and further damage caused by such measures.\textsuperscript{501} Personal injuries are high ranked based on the HNS Convention, they include damage suffered either on board or outside the NHS ship. According to the HNS Convention, personal injury claims have priority over other claims.\textsuperscript{502} For this propose even if the damage exceeds the amount which is established as financial limit of the Fund (250 million units), the personal injury claims have priority up to two-thirds of the total amount of compensation.\textsuperscript{503} In addition, when a State Party does not fulfil its obligations under the HNS Convention, no compensation for any incident shall be paid by the HNS Fund for damage in the territory, other than personal injury.\textsuperscript{504} Thus, personal injury can be compensated by the NHS Fund, even if the regulation of the HNS Convention has not been complied with by the state party or by the owner.

The property damage and economic losses might be considered under HNS Convention if the accident caused damage to property outside of the NHS ship, not inside.\textsuperscript{505} Thus, property damage on board of the ship is not subject to the HNS Convention. Loss of profit from the contamination of environment is also taken into account. Thus, even pure economic loss (such as loss of income in fishing and tourism) is also included in the scope of the damage under the HNS Convention. Environmental damage caused by hazardous and noxious substances is included in the HNS Convention, although with some exceptions. First environmental pollution which is covered by the CLC and radioactive substances are excluded from the scope of the HNS Convention. Second, the compensation for environmental damage is limited to the costs of actual reasonable measures for reinstatement of the polluted area. Finally as mentioned earlier, the costs of preventive measures and further loss or damage caused by preventive measures are included in the HNS Convention. However, these measures as well as other matters are subject to the regulations of the competent court.

5.4.1.8. Compulsory Insurance

The potential insolvency which might lead to the incapability of the ship owner to compensate victims, therefore compulsory insurance has been provided by the HNS Convention. According to Article 12 of the HNS Convention, the owner of a HNS ship is required to take insurance, or to maintain other acceptable financial securities, to cover sums fixed by applying the limits of liability. On the other hand, the State of the ship's registry or any relevant state party should issue a certificate attesting that insurance or other financial security is in force in accordance with the provisions of the HNS Convention.

The issuance of the insurance certificate by the state party is an important step for the assurance of compulsory insurance by the ship owner. First, since the insurance certificate template has been laid down in Annex I of the HNS Convention and requires uniform information for all the ships, the necessary information concerning the ship, the owner, type and duration of the security can be easily accessed.\textsuperscript{506} Second, a State Party shall not permit a ship under its flag to which this article applies to trade unless a certificate has been issued under HNS Convention.\textsuperscript{507} This rule constrains the ship owner to establish insurance under the provision of the HNS Convention for trading with the state party to the HNS Convention. Third, since the certification for insurance should be issued by the state party’s authority, the burden of verifying the compliance of insurance or other security with the regulation of the

\textsuperscript{501} Article 1 of the HNS Convention.  
\textsuperscript{502} Article 11 of the HNS Convention.  
\textsuperscript{503} Articles 11 and 14 of the HNS Convention.  
\textsuperscript{504} Article 21bis of the HNS Convention.  
\textsuperscript{505} Article 1 of the HNS Convention.  
\textsuperscript{506} Article 12 of the HNS Convention.  
\textsuperscript{507} Ibid.
HNS Convention falls into responsibility of the respective state party. No liability for state party has been envisaged concerning failures it would have committed in the verification of the compliance of the insurance or other security with the provisions of the HNS Convention. However, in case the insurer or the owner is financially incapable, the HNS Fund will pay the compensation. They might to some extent undermine the efficiency of the compulsory insurance.

Claimants might bring any claim directly against the insurer or other person providing financial security for the ship-owner's liability for damage. The insurer is entitled to invoke the defences which the ship-owner might invoke, even if the ship-owner is not entitled to the limitation of liability. However, the insurer is not allowed to invoke the bankruptcy or winding up of the ship-owner. In addition, the insurer can claim that the damage resulted from the intentional misconduct of the ship-owner, but cannot call on other defences.\(^\text{508}\)

5.4.1.9. Applicability in time

One of the issues which might limit the scope of liability is the limitation of the action in time. The HNS Convention has considered this question as follows. In the first tier, the rights to compensation against the ship owner have to be brought within three years from the date when the claimant knew or ought reasonably to have known of the damage and of the identity of the owner. However, some types of environmental contamination might only be discovered after years. For this purpose, in the second tier, ten years after the date of the incident has been established as utmost time for the action against owner or the Fund.\(^\text{509}\)

5.4.1.10. Compensation mechanisms

The liability of the owner has been limited under the HNS Convention. For this purpose, a specific mechanism has been set up by the HNS Convention for compensation of the damage. If the ship owner enjoys from the limitation of liability, the owner shall constitute a fund for the total sum representing the limit of liability before the competent court or other competent authorities of any one of the States Parties whether that action against the owner has been brought or not.\(^\text{510}\) With a constitution of the fund all the claim against the owner should be only exercised before the fund.\(^\text{511}\) The aforementioned fund might be established either by depositing the sum or by providing a financial guarantee, according to the applicable law of the court or other competent authority.

All the claims shall be brought before the established fund. If the owner or any other persons has paid compensation for damage before establishment of the fund, they will be subrogating in the rights of the claimant which has been compensated by him. Given the compulsory insurance under the HNS Convention, the insurer or other person providing financial security is entitled to constitute a fund in accordance with the regulation of the HNS Convention, even if the owner is not entitled to a limitation of liability.\(^\text{512}\) This will reduce the administrative cost of the compensation.

Generally the action against the HNS Fund for compensation shall follow before a court having jurisdiction in respect of actions against the owner or the owner's insurer. In case that

\(^{508}\) Ibid.

\(^{509}\) Article 37 of the HNS Convention.

\(^{510}\) Article 9 of the HNS Convention.

\(^{511}\) Article 10 of the HNS Convention.

\(^{512}\) Article 9 of the HNS Convention.
the ship owner is exempted from liability, legal action against the HNS Fund must be brought in a court which would have been competent if the ship owner had been liable. When the owner has not been identified yet, the action will be brought against the Fund only in States Parties where the damage occurred.\textsuperscript{513} Therefore, the mechanism of compensation under the HNS Convention has been based on the establishment of the fund, primarily according to the regulation of the competent court and by the owner or insurer. This procedure shall be validated by the respective state party. Nonetheless, if the amount of the damage exceeds the liability of the owner or if any other reasons which shift the liability of compensation the damage to the HNS Fund are present, the competent court shall judge about the compensation by the HNS Fund. Thus, the action against the HNS Fund, can only be brought before the competent court and through litigation in the tort system.

It is necessary to mention that after initiating any proceedings under the regulation of the HNS Convention, each party to the litigation is entitled to notify the HNS Fund of the proceedings. As a result of the notification which should be done according to the national law of the court, the HNS Fund has a position to intervene as a party to the proceedings. Accordingly the final judgment in this condition will be binding upon the HNS Fund, even if the HNS Fund has not actually intervened in the proceedings.\textsuperscript{514}

5.4.1.11. Jurisdictional issues

Claimants can take legal action in a court in the respective state party which has jurisdiction over the damage. The competent court will have exclusive jurisdiction to consider all matters relating to damage and compensation. The fund will also be established before the competent court or other competent authority of the state party which has jurisdiction over the case. According to Article 38 of the HNS Convention each state party has the jurisdiction, if the accidents or the preventive measures have been caused in the territory including territorial sea of that state. Since, according to Article 3 of the HNS Convention, contamination of the environment caused in the exclusive economic zone of a State Party has been included in the scope of the application of the HNS Convention, if such type of damage has been caused in the Exclusive Economic Zone of a state party, the respective state party has jurisdiction over the case.\textsuperscript{515}

5.4.1.12. Conclusions HNS Convention

It can be concluded that the HNS Convention covers damage which might result from a HNS ship. In hierarchy of damage priority is given to personal injury, in addition to putting an emphasis on the inclusion of the cost of preventive measures. Moreover, the owner is strictly liable and members of the crew are exempted from the liability, except for cases of intent or reckless actions. The strict liability regime has been complemented with a compulsory insurance to the amount of the limitation. Moreover, in case the operator has not been held liable the cost of damage might be paid by the HNS Fund which is established as a second tier compensation regime. Thus, the damage can be compensated by the insurance or via the HNS Fund mechanism.

\textsuperscript{513} Article 39 of the HNS Convention.
\textsuperscript{514} Article 38 of the HNS Convention.
\textsuperscript{515} Articles 3 and 38 of the HNS Convention.
5.4.2. Protocol on Civil Liability and Compensation for Damage Caused by the Transboundary Effects of Industrial Accidents on Transboundary Waters (2003 Civil Liability Protocol)

5.4.2.1. Brief summary of the regime

Under auspices of the United Nations Economic Commission for Europe (UNECE), five environmental treaties have been negotiated, all of which are now in force. With respect to compensation for transboundary damage, and recalling the relevant provisions of the Convention on the Protection and Use of Transboundary Watercourses and International Lakes and the Convention on the Transboundary Effects of Industrial Accidents (1992), the Civil Liability Protocol was adopted on the 21st of May 2003. However, this protocol is not yet in force. According to Article 1 of the Civil Liability Protocol, its objective is “to provide for a comprehensive regime for civil liability and for adequate and prompt compensation for damage caused by the transboundary effects of industrial accidents on transboundary waters.”

Various problems may arise in case of transboundary damage. For example, the affected state might not have been informed about the adverse environmental impact of certain activities. Also, even after being aware of this adverse impact, affected states may face obstacles to start litigation against polluting states. Also, there is no harmonized definition of the concept ‘environmental damage’. The aforementioned Conventions include some provisions on damage definition, prevention of damage, and cooperation among respective states in the context of transboundary pollution, while provisions on liability for and compensation of transboundary damage are laid down in the Civil Liability Protocol.

The Parties to the Protocol have accepted the polluter pays principle as a basis for the liability regime, taking into account that this principle is generally accepted in international environmental law. Based on the polluter pays principle, operators are strictly liable for the damage caused by industrial accidents (Article 4(1)). Furthermore, a fault-based liability might be applied to other persons such as servants or agents of the operator, if they cause or contribute to damage by their “wrongful, intentional, reckless or negligent acts or omissions” (Article 5). Following an accident, the operator shall take all reasonable measures for mitigation of damage according to the applicable domestic law and other relevant provisions of the Conventions. The liability of operators is financially limited, based on the types of substances and their quantities (Article 9 and Annex 2). The Protocol contains a provision on financial security (Article 11).

---

516 For more information see: http://www.unece.org/env/welcome.html.
517 In particular Article 7 of the former and Article 13 of the latter.
520 See the preamble to the Civil Liability Protocol.
521 Industrial hazardous activities are listed in the annex of the Convention on the Transboundary Effects of Industrial Accidents.
5.4.2.2. **Basis of liability**

The Protocol applies to damage caused by the transboundary effects of an industrial accident on transboundary waters, and only to damage suffered in a country other than that where the industrial accident has occurred.\(^{522}\) With that in mind, Article 4 of the Protocol imposes strict liability on operators for damage caused by an industrial accident.

The operator can escape liability if he or she can prove that the accident resulted from “an act of armed conflict, hostilities, civil war or insurrection”, or if it is “the result of a natural phenomenon of exceptional, inevitable, unforeseeable and irresistible character”. Furthermore, no liability shall be attached to the operator if the damage is “[w]holly the result of compliance with a compulsory measure of a public authority of the Party where the industrial accident has occurred” or is “wholly the result of the wrongful intentional conduct of a third party”.\(^{523}\) The exclusion from liability according to the abovementioned reasons would be granted only if the operator has been taking appropriate safety measures according to the applicable law.\(^{524}\)

Moreover, without prejudice to the strict liability regime, a fault-based liability might be imposed on persons who have caused or contributed to the accident by their wrongful, intentional, reckless or negligent acts or omissions.\(^{525}\) Hence, strict liability will be imposed on operators to the extent that damage has not been caused by the wrongful act of other persons. In other words, the operator and the operator’s agents or servants are identified as separate persons in the Protocol. When taking into account also the right of recourse defined in Article 7 of the Protocol, and the fault-based liability for other parties than the operator in Article 5, one could argue that the basis of liability is not only strict liability, but strict liability and negligence as complementary regimes.

5.4.2.3. **Liable persons**

The concept ‘operator’ has been defined in Article 1(e) of the 1992 Convention on the Transboundary Effects of Industrial Accidents as “any natural or legal person, including public authorities, in charge of an activity, e.g. supervising, planning to carry out or carrying out an activity”. There is no separate definition of this concept in the Civil Liability Protocol; but it can be deduced that operators can be private entities as well as a State-owned companies.\(^{526}\)

According to Article 4 (3) of the Protocol, if a victim has “by his or her own fault caused the damage or contributed to it, the compensation may be reduced or disallowed having regard to all the circumstances”. If no fault has been proven, the operator will be held strictly liable. However, as was stated above, if the accident was caused as result of compliance with the compulsory measures of public authorities, the operator will not be held liable. The question then arises whether the State concerned would be held liable in such cases. Article 12 of the Protocol somewhat answers this question, by stating that “[t]he Protocol shall not affect the rights and obligations of the Parties under the rules of general international law with respect to the international responsibility of States”.

\(^{522}\) Article 3 of the Civil Liability Protocol.

\(^{523}\) Article 4 (2) of the Civil Liability Protocol.

\(^{524}\) Ibid.

\(^{525}\) Article 5 of the Civil Liability Protocol.

\(^{526}\) Article 11 of the Protocol explicitly considers also the financial security of State-owned operators.
In cases that two or more operators are involved in one accident, the claimant has the right to seek full compensation for the damage from any or all of the operators liable. If one of the operators proves that only part of the damage was caused by an industrial accident within its responsibly, that operator would be held liable only to the extent of his or her responsibly (Article 4 (4)). Furthermore, the person liable may be entitled to a right of recourse against any other person also liable under the Protocol, e.g. pursuant to the law of the competent court or based on contractual arrangements.  

5.4.2.4. Damage covered

Loss of life or personal injury, property damage other than the liable person’s property, economic losses, costs of measures of reinstatement of the impaired transboundary waters, and costs of response measures have all been included by the Protocol in its definition of ‘damage’. The amount of damage is limited (see further below). No priority has been given to personal injuries. Thus, in cases where the aggregate amount of damage exceeds the financial limits defined in the Protocol, the compensation may have to be shared between different victims and types of damages (depending on the interpretation of the competent court).

Property damage is not specifically defined, which implies that all (transboundary) property damage resulting from an accident would be taken into account, except for the liable person’s own property damage. Economic losses refer to a loss of income which is directly derived from an impairment of a legally protected interest in any use of the transboundary waters for economic purposes, which is incurred as a result of impairment of the transboundary waters, taking into account savings and costs.

Environmental damage that can be compensated in the context of this Protocol relates only to damage caused by contamination of transboundary waters. This means more particularly the cost of measures of reinstatement of the impaired transboundary waters, limited to the costs of measures actually taken or to be undertaken. The aim of the compensation is to reinstate or restore damaged or destroyed components of transboundary waters to the conditions that would have existed had the industrial accident not occurred. Also the costs of response measures (to prevent, minimize or mitigate possible loss or damage or to arrange for environmental clean-up) are taken into account, which include “any loss or damage caused by such measures, to the extent that the damage was caused by the transboundary effects of an industrial accident on transboundary waters”.

The scope of the Protocol encompasses the damage caused by industrial accidents on transboundary waters. The concepts ‘industrial accident’ and ‘transboundary waters’ are defined in the respective Conventions. “Industrial accident” means “an event resulting from an uncontrolled development in the course of a hazardous activity”. Such an accident might

---

527 For details see Article 7 of the Civil Liability Protocol.
528 Article 2 of the Civil Liability Protocol.
529 Article 2(iii) of the Protocol
530 Ibid.
531 Article 2(iv) of the Civil Liability Protocol.
532 Article 2(v) of the Civil Liability Protocol.
534 In turn, ‘hazardous activity’ means “any activity in which one or more hazardous substances are present or may be present in quantities at or in excess of the threshold quantities listed in annex I and which is capable of causing transboundary effects on transboundary waters and their water uses in the event of an industrial accident”. See Article 2 (f)-(g) of the Civil Liability Protocol.
have occurred in an installation, during transportation on the site of a hazardous activity; or during off-site transportation via pipelines. Again, only damage caused in a State other than the State or origin is included.\(^{535}\)

As past experience with industrial accidents has shown,\(^{536}\) accidents related to a hazardous activity as referred to in the Protocol and Conventions may lead to high numbers of personal injuries, environmental damage and economic losses. The Protocol, however, includes financial limits on the amount of compensation due. This limitation of liability only applies to the strict liability of the operator, defined in Article 4 of the Protocol, and not to the fault-based liability regime that is the subject of Article 5.\(^{537}\) The financial caps are related to different types of hazardous substances and hazardous activities, defined in Annex I and Annex II of the Protocol. For example, a distinction is made between substances which are ‘very toxic’, ‘toxic’ or ‘dangerous to the environment’, depending on particular physical and chemical properties specified in Annex I.\(^{538}\) Hazardous activities are grouped in three different categories. Category A includes hazardous activities in which quantities of hazardous substances do not exceed four times the threshold quantities specified for each hazardous substance (very toxic, toxic, or dangerous to the environment). The liability of damage caused by the substances in the category A is limited to 10 million units of account. Category B contains quantities of hazardous substances exceeding four times the threshold quantities, and benefits from a liability cap of 40 million units of account. Category C encompasses quantities of hazardous substances in which one or more hazardous substances are or may be present in quantities at or in excess of the threshold quantity specified. The liability of damage caused by the substances in the category C is limited to 40 million units of account.\(^{539}\)

This limitation of liability may allow insurability of such damage, especially when taking into account the provisions on financial security which are also defined in Annex II of the Protocol (respectively 2.5, 10 and 10 million units of account; see further below). However, damage exceeding the amount of financial liability is not compensated via the provisions of the Civil Liability Protocol. Even if the damage resulted from a personal act or omission by the operator, he or she can enjoy limitation of liability.

### 5.4.2.5. Exclusions and defences

See section 5.4.2.2 above, where we discussed Article 4 (2) of the Protocol in detail.

### 5.4.2.6. Causation

According the Protocol, the operator shall be held strictly liable for the damage caused by the transboundary effects of an industrial accident on transboundary waters. The burden of proof (regarding the causal link between the damage and activities by particular hazardous industries) lies in principle with the plaintiff. Two questions concerning the establishment of a causal link between the damage and the industrial hazardous activities seem to be relevant in this respect. First, the recognition of the industrial site as one which falls under the jurisdiction of the Conventions and Protocol; and second, the establishment of a causal link

---

\(^{535}\) Article 3 of the Protocol


\(^{537}\) Article 9 of the Civil Liability Protocol.

\(^{538}\) For details see Annex I and II of the Civil Liability Protocol.

\(^{539}\) Annex II part one of the Protocol
between the damage caused and the hazardous activity. The Conventions contain some provisions on the identification of hazardous industries and duties of respective parties to notify each other of any such proposed or existing activity.\(^{540}\) In addition, by the establishment of the Industrial Accident Notification System, in case of an accident the origin state shall notify the affected state at appropriate levels.\(^{541}\)

‘Transboundary impact’ is meant to include any significant adverse effect on the environment resulting from a change in the conditions of transboundary waters caused by a human activity, which includes effects on human health and safety, flora, fauna, soil, air, water, climate, landscape and historical monuments or other physical structures.\(^{542}\) According to this definition, adverse impact is a relative concept, the exact meaning of which may differ when different standards are taken. To fill this gap, the Convention on the Protection and Use of Transboundary Watercourses and International Lakes prescribes bilateral or multilateral cooperation between Riparian Parties in order to eliminate contradictions and to adapt arrangements e.g. for drawing up inventories of pollution sources, elaborating emission limits and monitoring transboundary water quality.\(^{543}\)

Some questions might arise in relation to damage which is caused by more than one operator. The protocol prescribes joint liability in such cases, by holding all involved operators liable for the damage caused without determining the share of each individual party. However, if the operator can prove that only part of the damage was caused by an industrial accident, he or she would be liable only for that part of damage.\(^{544}\)

### 5.4.2.7. Applicability in time

Article 10 of the Civil Liability Protocol sets the time limit of liability. Similar to most environmental treaties, two time limits are defined there. In the first tier, the claim should be brought within three years from the date when the claimant knew or ought reasonably to have known of the damage. In the second tier, the claim should be brought within 15 years from the date of the industrial accident.

In case of a series of occurrences having the same origin, the last of such occurrences will be considered as the starting date of the time limits. Where the industrial accident consists of a continuous occurrence, time limits shall run from the end of that continuous occurrence.

### 5.4.2.8. Relation with regulation

Both Conventions underlying the Protocol include provisions on the prevention, mitigation and reinstating of transboundary adverse impacts.\(^{545}\) Operators are excluded from strict liability only in the cases defined in Article 4 of the Protocol (and discussed above under 5.4.2.2). This includes situations of force majeure and compliance with a compulsory

---

\(^{540}\) Article 4 of the Convention on the Transboundary Effects of Industrial Accidents.
\(^{541}\) Article 10 of the Convention on the Transboundary Effects of Industrial Accidents.
\(^{542}\) Article 1 of the Convention on the Protection and Use of Transboundary Watercourses and International Lakes.
\(^{543}\) Article 9 of the Convention on the Protection and Use of Transboundary Watercourses and International Lakes.
\(^{544}\) Article 4 of the Civil Liability Protocol.
\(^{545}\) See e.g. Articles 2, 3 and 9 of the Convention on the Protection and Use of Transboundary Watercourses and International Lakes; and Articles 3, 4, 6 and 7 of the Convention on the Transboundary Effects of Industrial Accidents.
measure, where the operator still has to prove that the accident occurred “despite there being in place appropriate safety measures”.

The financial limits discussed in section 5.4.2.4 above and included in Annex II of the Protocol are not related to regulation but to the nature of the hazardous substances and the activities.

5.4.2.9. Financial security and compensation mechanisms

Operators shall ensure that they have financial security covering at least the minimum limits specified in Annex II of the Protocol: 2.5 million units of account for Category A hazardous activities, and 10 million units of account both for Categories B and C. The type of financial security has not been prescribed; Article 11 in that respect refers to “insurance, bonds or other financial guarantees including financial mechanisms providing compensation in the event of insolvency.” In addition, State-owned operators can fulfil their obligation by a declaration of self-insurance.

The minimum limits of financial securities have been established at one-fourth of the liability caps. The limits shall be reviewed by the Meeting of Parties on a regular basis taking into account the risks of hazardous activities as well as the nature, quantity and properties of the hazardous substances that are present or may be present in such activities. However, as apparently no mechanism is included in the Protocol that enables the respective States to verify whether appropriate financial security is in place, there may be a risk that operators underestimate this issue.

Claimants may file a claim directly against the provider of financial security. However, this does not relieve the person liable under Article 4 from being joined in the proceedings. The insurer and insured can make use of deductibles or co-payments, but the failure of the insured to pay any deductible or co-payment shall not be a defence against the person who has suffered the damage. Furthermore, bringing suit directly against e.g. an insurer can be excluded ex ante by means of written notification by the respective Party at the time of signature, ratification, approval of or accession to the Protocol.

In principle, the establishment of the right for the claimant to bring suit directly against an insurer might be considered as a rule which facilitates compensation, whereas the exemption clause to this rule might increase the administrative cost of compensation mechanism. However, it should be noted again that the right of recourse has been established in Article 7 of the Protocol, also via contractual arrangements.

5.4.2.10. Rules of evidence

To the extent that this is relevant, see section 5.4.2.6 above.

546 For a definition of the categories, see Annex I and II of the Protocol or section 5.4.2.4 supra.
547 Article 11 (1) of the Civil Liability Protocol.
548 Article 11 (3) of the Civil Liability Protocol.
5.4.2.11. Jurisdictional and procedural issues

The Protocol contains Articles on competent courts (where the damage was suffered, where the accident occurred, or where the defendant is located), on arbitration, and on applicable law, but these are not relevant in the specific context of our study.

5.4.2.12. Conclusions 2003 Civil Liability Protocol and relevance to the Security Industry

The Civil Liability Protocol, which is not yet in force, establishes a strict liability regime for operators with respect to compensation for damage caused by the transboundary effects of industrial accidents on transboundary waters. This regime is complemented by a financial limitation of liability which, inter alia, may facilitate the insurability of such damage. However, the minimum amount of financial security prescribed by the Protocol is only one-fourth of the amount of the liability cap. A claimant can directly bring action against the insurer, unless a State opts out of this regime explicitly.

It might be concluded that the aim of the Protocol is to establish a liability regime which to some extent governs transboundary water industrial accidents. According to the UNECE website, the Protocol “will give individuals affected by the transboundary impact of industrial accidents on international watercourses (e.g. fishermen or operators of downstream waterworks) a legal claim for adequate and prompt compensation”. Also, it “fills one of the major gaps in international environmental legislation and solves the problem of uncompensated damage in neighbouring countries.” Nevertheless, since the adoption of the Protocol on 21 May 2003 only Hungary has ratified it and all other State Parties have not.

One reason might be the scope of the Protocol, which includes a wide range of industries. Another reason might be uncertainty concerning the effectiveness and practical usefulness of the Protocol (with its wide range of exclusions and possibilities to opt out of certain clauses).


5.4.3.1. Brief summary of the regime

Elaborating on Article 7 of the 1967 UN Outer Space Treaty, the 1971 Convention on International Liability for Damage Caused by Space Objects (Liability Convention) provides that a launching State shall be absolutely liable to pay compensation for damage caused by its space objects on the surface of the Earth or to aircraft. Furthermore, a launching State shall be liable for damage due to its faults in space. The Convention also provides for procedures for the settlement of claims for damages. Agreement on the Liability Convention was reached in the General Assembly in 1971 and the Convention entered into force in September 1972.

549 For details, see in particular Articles 13-18 of the Civil Liability Protocol.
550 http://www.unece.org/env/civil-liability/welcome.html. More potential benefits of the Protocol are listed there, including its expected effects on prevention of accidents.
552 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, adopted on 27 January 1967. Article 7 reads as follows: “Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the Moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air space or in outer space, including the Moon and other celestial bodies.”
5.4.3.2. Basis of liability

The Convention imposes absolute liability, which refers to a liability system without any defence or exclusion. Article 2 states that “[a] launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the Earth or to aircraft in flight.”

The Convention in Article 3 also introduces a negligence-based liability, by imposing liability on a launching State for damage due to its faults in space: “In the event of damage being caused elsewhere than on the surface of the Earth to a space object of one launching State or to persons or property on board such a space object by a space object of another launching State, the latter shall be liable only if the damage is due to its fault or the fault of persons for whom it is responsible.”

5.4.3.3. Liable persons (attribution of liability)

The Liability Convention refers to the concept of ‘launching States’. According to Article 1 of the Convention, the term launching State means: “(i) A State which launches or procures the launching of a space object; (ii) A State from whose territory or facility a space object is launched”. The term “launching” also includes attempted launching.

In Article 4 a system of joint and several liability is introduced with respect to all damage being caused elsewhere than on the surface of the Earth to a space object of one launching State or to persons or property on board such a space object by a space object of another launching State, and of damage thereby being caused to a third State or to its natural or juridical persons. In such case the first two States shall be jointly and severally liable to the third State. The burden of compensation per State depends on the extent to which each of the States were at fault (i.e. a system of proportional liability). If the extent of the fault cannot be established, the States will have to share the burden of compensation equally.

Joint and several liability is also imposed whenever two or more States jointly launch a space object and thereby cause damage (Article 5). The participating States in a joint launching may conclude agreements regarding the apportioning of liability among themselves, as long as this does not limit the right of the State where the damage occurs to be compensated.

5.4.3.4. Damage covered

In the preamble to the Convention, the need is recognized to ensure prompt payment of a full and equitable measure of compensation to victims of damage caused by space objects. The term “damage” is defined in Article 1 of the Convention, and refers to “loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations”. Hence, damages seem to relate to property damage and personal injury.

Article 12 adds to this that the amount of the compensation “shall be determined in accordance with international law and the principles of justice and equity, in order to provide such reparation in respect of the damage as will restore the person, natural or juridical, State

553 Liability Convention, Article 1 (b) and (c).
554 See furthermore Article 4 (1).
555 Liability Convention, Article 1 (a).
or international organization on whose behalf the claim is presented to the condition which
would have existed if the damage had not occurred.”

5.4.3.5. Exclusions and defences

There are no exclusions or defences. Article 6 (1) of the Convention states that exoneration
from absolute liability can only be granted if a launching State establishes that the damage
“has resulted wholly or partially from gross negligence or from an act or omission done with
intent to cause damage on the part of a claimant State or of natural or juridical persons it
represents.”

5.4.3.6. Causation

There are no special rules on causation.

5.4.3.7. Relation with regulation

Not applicable.

5.4.3.8. Financial security and compensation mechanisms

The Liability Convention does not provide for any special financial security or compensation
mechanism.

5.4.3.9. Rules of evidence

Not applicable.

5.4.3.10. Jurisdictional and procedural issues

There are no relevant issues to be discussed in this respect.

With respect to the filing of a claim, the Convention provides that States suffering damage
may present – through diplomatic channels - to a launching State a claim for compensation. If
the claimant State does not maintain diplomatic relations with the launching State concerned,
it may request another State to present its claim to that launching State or it may present its
claim through the Secretary-General of the United Nations (Articles 8 and 9).

The claim must in principle\textsuperscript{556} be presented no later than one year after the date of the
occurrence of the damage or the identification of the launching State which is liable (Article
10(1)). Articles 14-20 of the Convention provide for settlement procedures if diplomatic
negotiations do not work.

\textsuperscript{556} See for exceptions Article 10 (2) and (3).
5.4.3.11. Conclusions Space Liability Convention and relevance to the Security Industry

The concept of absolute liability without any defence or exclusion for damage caused by space objects on the surface of the Earth or to aircraft in flight is very interesting. However, to our knowledge the Convention has never been applied. Also, the Convention does not include any provisions on financial security or insurance.

Another striking aspect of this Convention is the fact that liability is attributed to the state and not to operators. It has been indicated in the legal literature that this is the only treaty where states are directly held liable. 557

5.5. Concluding observations

At the end of this chapter where we analyzed potential analogies between the security industry on the one hand and international treaties dealing with civil aviation, nuclear liability and environmental liability on the other hand, we will draw some conclusions. Having analyzed seven different international treaties which all contain specific liability rules, we will first compare the liability regimes in the specific treaties (5.5.1). Subsequently, we will examine to what extent these treaties may have some relevance for the security industry (5.5.2). Finally, we will address the question whether some lessons can be drawn from the study of these international treaties for a future liability regime for the European security industry (5.5.3).

5.5.1. Liability regimes

The seven liability regimes addressed in this chapter can be categorized into three groups. The first group of conventions relates to civil aviation, more particularly the Rome Convention on ‘damage caused by foreign aircrafts to third parties on the surface’ and the Montreal Convention on ‘international carriage by air’. The second set of conventions deals broadly with nuclear liability. After the discussion of these nuclear liability conventions we presented the international conventions dealing with civil liability for and compensation of damage caused by oil pollution, more particularly the Civil Liability Convention for Oil Pollution Damage (CLC) and the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (Fund Convention). The third set of conventions dealt with other relevant treaties, whereby we selected those treaties that also have provisions on liability: the International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by See (HNS Convention), the Protocol on Civil Liability and Compensation for Damage Caused by the Transboundary Effects of Industrial Accidents on Transboundary Waters (Civil Liability Protocol) and finally the admittedly rather exotic UN Convention on International Liability for Damage Caused by Space Objects (also referred to as the 1971 Liability Convention).

When comparing the liability regimes in these seven conventions based on the common format for the analysis of liability regimes we could summarize the main features as follows:

557 See e.g. Sands and Peel 2012.
### Scheme 2: comparison of liability regimes in international treaties

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Rome</th>
<th>Montreal</th>
<th>Nuclear</th>
<th>Oil</th>
<th>HNS</th>
<th>Protocol</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis</td>
<td>SL²⁵⁸</td>
<td>SL</td>
<td>absolute</td>
<td>SL</td>
<td>SL</td>
<td>SL</td>
<td>SL</td>
</tr>
<tr>
<td>Liable persons</td>
<td>operator; liability of others not excluded</td>
<td>air carrier, but liability of others possible as well</td>
<td>operator</td>
<td>ship owner</td>
<td>ship owner</td>
<td>operator</td>
<td>launchin g state</td>
</tr>
<tr>
<td>Damage</td>
<td>cap</td>
<td>cap</td>
<td>cap</td>
<td>cap</td>
<td>cap</td>
<td>cap</td>
<td>cap</td>
</tr>
<tr>
<td>Defence s</td>
<td>armed conflict; not natural disasters / terrorism</td>
<td>not terrorism / natural disaster</td>
<td>armed conflict and civil war; natural disaster not</td>
<td>armed conflict and civil war; not natural disaster</td>
<td>war ; exception al natural disasters</td>
<td>war ; exception al natural disasters</td>
<td>-</td>
</tr>
<tr>
<td>Relation with regulation</td>
<td>damage from passage of aircraft in conformity with regulation: no liability</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Financial security</td>
<td>mandatory security</td>
<td>mandatory security</td>
<td>mandatory security</td>
<td>mandatory security</td>
<td>mandatory security</td>
<td>mandatory security (limited)</td>
<td>-</td>
</tr>
<tr>
<td>Additional funding</td>
<td>-</td>
<td>-</td>
<td>state intervention</td>
<td>fund</td>
<td>fund</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

5.5.2. **Relevance for the security industry**

The conventions discussed above are relevant in the sense that they often channel liability to particular operators. In some cases this constitutes an exclusive channelling. This is for example the case in the CLC, which channels liability in principle exclusively to the ship owner. Hence, the liability of others (like the security industry) is excluded. The same seems to be the case in the HNS convention which equally channels liability to the ship owner. Also in cases where involvement of the security industry may be more likely, like in the nuclear area, there is a strong reliance on channelling to the operator of the nuclear power plant. Exceptions to the channelling are quite difficult and would only occur e.g. if there would be an agreement between the operator of the nuclear power plant and the third party (presumably the security industry). However, it is unlikely that the security industry would voluntarily accept liability in case of a nuclear accident. In that sense it can be held, as was mentioned above, that exclusive channelling to e.g. the operator of a nuclear power plant or a ship owner (like in the case of the CLC and HNS Convention) in fact shields the security industry from liability. Furthermore, in the case of the Convention on International Liability for Damage Caused by Space Objects, liability is attributed to the “launching states”.

²⁵⁸ ‘SL’ means strict liability.
In some cases the channelling is not exclusive and other parties can still be held liable. This is, for example, the case in the Montreal Convention on international carriage by air. However, the persons who could be held liable are also addressed in a limited manner in the convention, for example indicating that liability would be possible against other agents of the contracting or actual carrier. A similar provision can be found in the Rome convention where channelling also is not exclusive. Moreover, both conventions still have the possibility of a right of recourse against other liable parties.

It is, however, important to note that defences in international conventions are relatively limited. For example in the case of the Rome and Montreal conventions terrorism or natural disasters do not constitute a ground of excuse or justification. This in a way is (again) reassuring for the security industry since it means that the exclusive channelled (strict) liability will still apply to the designated operators in the international conventions, again limiting the likelihood that on the basis of those conventions one would call on the liability of the security industry. That would in fact only be possible in case of recourse and then only in those conventions that allow for such a recourse.

Summarizing, the study of these liability regimes in the international treaties do not create a specific liability regime for the security industry; to the contrary it seems that the exclusive channelling to others rather provides a shield from liability for the security industry.

5.5.3. Lessons for a future liability regime for the European security industry?

We can now address the question whether the seven conventions that we have studied in more detail in this chapter provide interesting features that could be taken into account for a potential EU liability regime for the security industry. As we argued also at the end of Chapter 3, we have to be careful here. After all, the pros and cons of various options will be analysed in further detail in Chapter 8 when addressing legal and technical options for implementing a feasible third party liability regime in the EU.

A first interesting feature, when looking at the table that summarized the liability regimes is that all treaties we examined are based on strict liability. This is to some extent not surprising since all treaties apply to so-called hazardous activities and strict liability often applies to ultra-hazardous activities.

Another important feature already mentioned was the channelling of liability to the operator. Especially when discussing the international conventions with respect to nuclear liability and marine oil pollution liability, we argued that an exclusive channelling of liability can undoubtedly be considered as beneficial to the security industry. After all, when only the operator (e.g. of a nuclear power plant) is indicated as liable person this automatically removes the threat of liability from the security industry. However, one should be careful by implying from the mere fact that many international conventions use this channelling of liability, that it would therefore also be a useful or interesting device for a future EU liability regime for the security industry. Our discussion of the nuclear liability conventions and the marine pollution conventions already taught us that such channelling of liability is highly criticised in the literature. The main problem is that when liability is exclusively channelled to

559 Some of the regimes also include an additional fault-liability regime; see e.g. the 2003 Civil Liability Protocol and the Convention on International Liability for Damage Caused by Space Objects (for faults in space only). See sections 5.4.2 and 5.4.3 supra.
560 See 5.2.11.
561 See 5.3.11.
one liable operator this automatically excludes liability of all others who also could have contributed to the accident risk. If one believes that liability rules also provide incentives for prevention (as is argued, e.g., in law and economics literature) that may not be a desirable effect. Indeed, channelling may remove the incentives for prevention for others than the single operator to whom the liability risk is channelled.

Similar arguments apply with respect to another feature that was apparent in six out of the seven international conventions discussed above, being that liability is always limited. Indeed, most international conventions apparently pay an important price for the strict liability of the operator, i.e. a financial cap is put on the liability of the operator. But again, literature with respect to the nuclear and marine pollution conventions was very critical with respect to the financial cap on liability. The criticism is directed on the one hand to the fact that the operator will only have incentives to prevent an accident to the amount of the limited liability. A financial cap could hence reduce the incentives for prevention. On the other hand, to the extent that the actual damage could be substantially larger than the capped liability, victims would remain uncompensated. This leads to a third type of criticism, being that a financial cap on liability de facto allows operators to externalise harm to society. From an economic perspective a financial cap constitutes in fact a subsidy to industry which may be problematic. Similar criticisms were also formulated with respect to yet another interesting feature in both the nuclear liability and marine oil pollution conventions, being that additional funding is provided. In the case of the nuclear conventions this additional funding is provided by the installation state (the so called second layer) or by all signatory states (the so called third layer). This state intervention is heavily criticized in the literature, arguing that public funds are used to compensate victims, subsidising once more the nuclear industry. That effect is not present in case of the marine pollution conventions. The International Oil Pollution Compensation Fund is financed through contributions by oil receivers and the same is the case for the HNS Fund which is equally financed by industry. Given the criticisms on those devices this could constitute an important lesson for a future liability regime for the EU security industry: the literature addressing nuclear liability and the liability for marine oil pollution strongly doubts the usefulness of a financial cap on liability, criticizes exclusive channelling and the provision of additional funding through the public purse.

There is yet one additional important feature that is apparent in six out of the seven international treaties we discussed, being that the operators that are held exclusively liable according to the conventions also need to show mandatory insurance. That constitutes an important difference with the comparable EU legislation that we discussed in chapter 3. In none of the three EU liability regimes (ELD, product liability and auditors’ liability) was there a duty to provide financial coverage, although this has been discussed. The overview of the conventions in this chapter shows that, apparently, at the international level the introduction of a duty to provide financial security in order to be able to meet the strict liability from the conventions seems to be the state of the art and could be considered as “best practice”. As will be argued in Chapter 8 below, there are strong economic reasons to introduce a strict liability regime only when solvency guarantees can be provided.

The liability regimes discussed in this chapter moreover nicely show that at the policy level a broad set of options can be provided to operators to provide proof of their solvency. This should hence not necessarily be limited to insurance. For example, the Rome Convention and the Civil Liability Protocol refer to a variety of financial security mechanisms such as cash deposits, bank guarantees and guarantees by the contracting state. These are interesting examples if one were to consider the introduction of a duty to provide financial security to cover the liability.
Chapter 6 Analysis of legal practices by industries exposed to analogous risks and by their insurers

In this chapter we will turn the focus to the question what practices industries follow that are exposed to analogous risks as the security industry and that may also develop techniques to limit their risk exposure.

On the one hand this chapter will address the theoretical benefits of particular techniques of limiting liability exposure; this theoretical exposé will of course be useful especially when later in Chapter 8 recommendations will have to be formulated for a feasible third party liability regime for the EU security industry. On the other hand the approach will also be empirical, in the sense that we will try (to the extent possible) to examine which techniques are followed by industries in analogous high risk situations to limit their risk exposure.

Since this chapter crucially deals with insurance, we start with a section explaining the legal and economic background of insurance (6.1). This background is important for understanding the working of insurance in the remainder of this chapter.

With limiting the risk exposure we refer to different types of techniques. One is the possibility to put a financial cap on liability. Liability capping and exclusion schemes do exist in other high risk sectors, some of which were already discussed in Chapter 5. Some other liability capping tools will be discussed here in section 6.2. Next, an important issue for the security industry may be that, if they cannot statutorily limit their liability (for example through a cap), they may be interested in looking at instruments of risk spreading. Our working hypothesis is that the security industry may potentially be exposed to high liability risks and this hence raises the question how industry could cope with the disutility following from this high risk exposure. Again, these techniques of risk spreading will be analysed in analogous situations to the security industry since this may provide interesting lessons for dealing with spreading of liability risks in the EU security industry. One technique of risk spreading often used in high risk industries is the creation of risk sharing agreements or risk pools. The practice of risk spreading via shared risk pools will also be explored in section 6.2.

Another way of spreading risks is insurance. Experience with so-called catastrophic risks has taught that these catastrophic risks may be difficult to insure. Nevertheless, insurers have developed a variety of techniques to deal with risks even if these risks are of a catastrophic nature. The experience of insurers, reinsurers and especially public-private partnerships in the insurance of disasters may provide useful insights also for potential risk spreading possibilities in the area of liability of the security industry. First we will address a liability-related insurance scheme for disasters: the insurer approach towards man-made disasters and terrorism (6.3). However, since typically in the case of a terrorist attack a liable injurer cannot be identified or is insolvent, the insurance approach followed with respect to terrorism shows many similarities with the field of natural disasters. The last field we will therefore look at is how insurers have developed specific constructions to make insurable catastrophic risks, more particularly natural disasters like flooding. (6.4).

---

562 This corresponds to Work Package 4 of the Invitation to Tender.
6.1. Insurance: legal and economic background

This section discusses the legal approach of insurance companies towards man-made risk (terrorism and large scale industrial accidents with a chemical, biological, radiological, nuclear or explosive component) and natural disasters. The focus is on contractual features of liability policies, as well as case law pertaining to insurance claims due to man-made and natural disasters, including the position of insurers in these cases and the main reasoning that led to the outcome of the cases. Although the analysis centers on European cases and companies, a few other examples (the Bhopal disaster in India, the BP “Deepwater Horizon” oil spill in 2010) are briefly discussed.

Before discussing the way insurance manages risk, we first present a discussion of how insurance works and why it is desirable. This discussion is relevant to understanding risk management by insurers and the limits of insurance. Then, in the section on managing liability risks, we focus also on recent development in the area of insurance against the risks of terrorism.

Insurance is generally deemed desirable because it spreads risks. There are two type of risk spreading: spreading over time (inter-temporal) and spreading over persons (inter-personal). Corporations are generally believed to be in a substantially better position than any single individual to spread risks broadly.

6.1.1. Insurance’s risk – reducing effects

Insurance as an objective (or function) of civil liability has also been defended on grounds derived from insurance theory. In simple terms, insurance involves a choice to incur a small and certain loss (the premium) now in exchange for not being exposed to a larger, uncertain loss in the future. Like risk spreading generally, insurance is attractive to risk-averse persons (and risk-averse societies). More precisely, insurance meets needs in society because it shifts risks from persons with inferior risk-bearing capabilities to persons with superior risk-bearing capabilities.

The theory of diminishing marginal utility of money can explain insurance only in terms of inter-temporal and inter-personal risk spreading. However, insurance is a complicated mechanism for managing risk. In addition to risk spreading, insurance has important risk-reducing effects. Its risk-reducing effects, according to Priest, are likely to be far more significant than the risk-spreading effects. Insurance reduces risks in two ways: first, it reduces the underlying injury rate and, second, it reduces the effective cost of remaining injuries by lowering the magnitude of total risk. Since an insurance company aggregates many potential losses incurred by the insured pool, the law of large numbers makes the total loss to the insurance company highly predictable, as a result of which the insurance

---

563 See Calabresi 1970, p. 47-55. As Priest has pointed out, under this theory an incidental social ‘benefit’ of corporate-provided insurance is that it offers insurance coverage to consumers that would not otherwise obtain insurance. See Priest 1985.
564 There are two major kinds of liability insurance policies: occurrence policies and claim-made policies. Occurrence policies cover any claims arising out of events that occur during the policy period, irrespective of when the claim is brought. Claims-made coverage provides insurance against claims first made during the policy period. Occurrence policies, more so than claims-made policies, are subject to a “long tail”. See Spier and Haazen 1996; Spier 1998.
565 In addition to risk transfer and risk spreading, according to the American Law Institute reporters, insurance performs a “risk-allocation function by charging each policy holder in proportion to the risks the latter poses”, see American Law Institute 1991, p. 66-67; Priest 1987; Priest 1989.
566 Priest 1987.
company’s reserves for anticipated losses is much smaller than the total of all reserves of individual risk bearers and, thus, losses can be dealt with more efficiently. Insurance thus permits corporations to reduce or eliminate their reserves for anticipated losses so that their capital can be put to more efficient uses. In addition to risk aggregation, insurance employs risk segregation by defining risk pools and setting premiums according to the average level of risk brought to the pool. Both risk aggregation and risk segregation serve to reduce risk variance and, thus, insurance premiums. By segregating an individual into a risk pool with a sufficiently narrow range of exposures to risks, the insurance premium remains attractive to persons in the low end of the range. This technique will keep the risk pool intact. Once the disparity between the insurance premium and the exposure of the low-risk pool members becomes too great, the risk pool will unravel. Segregation reduces both pool risk and insurance cost, and, accordingly, adverse selection.

As noted above, insurance can help also to reduce the level of injuries actually suffered. This effect flows directly from the risk-segregation function of insurance. Through the size of the premium charged, insurance informs decisions as to whether and how much to engage in the covered activity: high risks are charged a high premium and thus there is an incentive to scale down the activity. As a result of extremely high premiums, very high-risk individuals may not be able to contract insurance and may refrain from engaging in the pertinent activity, which may make the activity safer. In addition, to the extent that insurance companies possess superior knowledge about risk reduction and bring this expertise to bear in their relations with insureds, insurance can also play a direct role in risk reduction. Insurance companies, for instance, may monitor the activities of insureds and require emission controls in situations in which they are efficient. Thus, in addition to possible benefits through increasing utility, insurance may result in increased efficiency through reduced total risk.

6.1.2. Insurance prerequisites

Not each and every risk can be insured. To be insurable, and for insurance to deliver the benefits discussed above, risks must meet certain prerequisites. The main requirements are the following. First, the risks to be insured must have a sufficiently probabilistic character. Insurability requires that risk is probabilistic either as to whether it will occur (e.g. a fire risk), or as to when it will occur (e.g. death). If there is no reliable information on whether or when, on average, damage occurs, insurability will be adversely affected. If the damage will likely or certainly occur, the aggregation advantages of pooling are not obtainable. As a related matter, risks must be sufficiently predictable and quantifiable in monetary terms. If the risk posed by any given pool of policy holders cannot be predicted with a reasonable degree of

---

567 The law of large numbers makes the total loss more predictable, (in simple terms, the law of large numbers states that where one has a pool, there is a spread in numbers and an average, and if one takes a sample from the pool, the larger the sample, the more likely it is that the average number in the sample will be identical to the average for the whole pool). Consequently, the reserves aggregated losses are less; than the total of individual reserves for non-aggregated losses. See Riegel, Miller and Williams Jr. 1976, p. 15-21; Marshall 1974.

568 The more precisely risks are segregated the more accurately premiums reflect the risk brought to the pool, the more broadly insurance is available in the society.

569 See Priest 1987.

570 As discussed below adverse selection refers to the phenomena that high-risk actors are more likely to purchase insurance than lower-risk actors.

571 Insurance’s risk-reducing effect can be counteracted by the “moral hazard” arising from insurance coverage. This issue is discussed in the section on risk spreading through pricing, below.

572 Insurance also provides a valuable function by monitoring the activities of the insured; see Freeman and Kunreuther 1997, p. 25.

573 The term risk denotes a specifiable probability of loss. Uncertainty, on the other hand, involves unspecifiable probability of loss.
confidence, insurance is impeded.\textsuperscript{574} If risks are entirely unpredictable in terms of chance and size of potential harm, they cannot be insured. On the other hand, the magnitude of risks and size of potential harm do not have to be fully understood and quantifiable. Insurers can handle some degree of uncertainty in this regard but there are limits. If the risk to be insured is the risk of being held liable for damages, the applicable rules govern the size and scope of the risk. This, in turn, means that the law itself must be sufficiently certain and precise. One particular risk seriously undermining insurability is the risk of retroactive changes in the law increasing the scope of liability, as insurers have not set premiums and policy conditions on the basis of such an expanded liability regime, but on the previous narrower regime. Thus, retroactive expansion of liability regimes, by definition, is uninsurable, since the relevant risk in this case is the risk of an unforeseeable court ruling, which: is very uncertain and not quantifiable. Note also that where the time lag between the relevant occurrence and the damage increases (i.e. long-tail damage), informational and causal uncertainties increase, retroactive changes in liability law become more likely,\textsuperscript{575} and the insurability of the risk decreases.

A further prerequisite is that the risks to be insured are statistically independent. Risks are statistically dependent if, when one insured suffers damage, the chance increases that another insured suffers damage. In the case of a nuclear war, many insureds would suffer damage at the same time, and thus these risks are statistically dependent. In insurance language, this risk is known as a ‘common factor’, which is one of two major portfolio risks.\textsuperscript{576} In the context of liability insurance, changes in the law present a common-factor risk.

A third requirement is that insurers must not be seriously restricted in managing and reducing threats to insurability. Two major threats are adverse selection and moral hazard. Adverse selection refers to the phenomenon that persons presenting higher than average (or median) risk are more likely to contract insurance than those presenting lower risk, where it is difficult or expensive for the insurer to distinguish between higher and lower risks. Adverse selection results from ineffective risk segregation.\textsuperscript{577} In the context of product liability, Epstein provides a striking example: ‘[T]he doctrine of allowing recovery for foreseeable misuse is fundamentally at cross purposes with any viable conception of insurance markets’.\textsuperscript{578} Legal uncertainty may aggravate adverse selection.\textsuperscript{579} Insurers can control adverse selection by defining their screening and selection procedures, including more sophisticated questionnaires, rejecting applicants presenting higher risks and applying more targeted policy conditions. Moral hazard increases risks for insurers in a different way. Moral hazard causes insureds (and courts!) to be less careful and to incur higher costs than they would have had they not been insured. To control moral hazard, insurers employ instruments such as deductibles, co-insurance, caps, exclusions, premium differentiation, bonus/malus mechanisms, and the like.

\subsection*{6.1.3 First- and third-party insurance

To understand the risk-spreading and risk-reduction functions of insurance, a sound understanding of the differences between two major types of insurance is required, i.e. first-party insurance and third-party or liability insurance.\textsuperscript{580} Both types of polices perform an

\begin{itemize}
\item \textsuperscript{574} See American Law Institute 1991, p. 67.
\item \textsuperscript{575} For an analysis of retroactivity issues in the product liability context, see Schwartz 1983, p. 813-828.
\item \textsuperscript{576} The second major risk is known as pricing function. See Tanega 1996, p. 117.
\item \textsuperscript{577} Priest 1987, p. 1548.
\item \textsuperscript{578} Epstein 1985, p. 645-669.
\item \textsuperscript{579} See American Law Institute 1991, p. 86.
\item \textsuperscript{580} For an overview of differences between first-party insurance and tort liability, see Cane 1999, p. 245-248.
\end{itemize}
insurance function and provide coverage for damage to a group of insureds. However, there are important differences between the two types of insurance. As discussed below, these differences affect the efficiency of the insurance function provided by each type of policy.

The differences between first- and third-party insurance arise from the fact that the pool of victims in a first-party context are the insureds themselves; while the victims in a liability context are third parties. To the context of first-party insurance, insurers have it direct contractual relationship with the victims. In the third-party (liability) insurance context, however, insurers do not contract with the persons that suffer-actual harm but with a group of other people that under the law can be made to bear the losses incurred by the victims. This has serious implications for the extent to which insurers are able to control the threats to insurance discussed above, i.e. adverse selection and moral hazard. Many of the measures that first-party insurance policies incorporate to control these risks are not available to liability insurers. For instance, while in a first-party context an insurance company call reject potential victims who pose increased risk (or charge them a higher premium), it cannot do so with respect to the persons suffering the loss in a third-party context; the liability insurer can control only the pool of insureds, not the pool of victims. Compared to the first-party insurer, the liability insurer’s ability to control adverse selection is significantly less, because it is harder and more expensive to assess risk only at the level of the insureds (not the victims) and achieve optimal risk segregation. Control of moral hazard is even more difficult, if not virtually impossible, for a liability insurer. To control moral hazard, first-party policies invariably provide for deductibles, co-insurance, caps, exclusions, premium differentiation, bonus/malus mechanisms, and the like. Third-party liability insurers can use these instruments but only in relation to the insureds, not in relation to the victims, who create most of the moral hazard.

A further problem that plagues third-party (liability) insurance arises from the fact that the insurance policy conditions in the liability context are not (or at least not exclusively) written by the insurer but by courts applying liability rules and the legislature. In construing liability standards, courts can effectively vary the policy conditions and expand the scope of insurance coverage. The courts’ control over policy conditions thus results in retroactively expanding coverage. Faure and Hartlief explain this as follows:

Retroactive application of new liability standards causes insurance problems because at the relevant point in time the insurer was not able to charge a premium for the unknown risk, to require preventive measures, and to reserve for the risk. 581

This issue is at the heart of the liability insurance crisis. In the USA, the American Law Institute has concluded that:

[H]eightened levels of legal uncertainty have been an important influence on the interaction of the tort and liability insurance systems and the related insurance crisis. 582

While risks present a specifiable probability of loss, uncertainty results in an unspecifiable probability of loss, and thus undermines insurability. Further, retroactive liabilities adversely affect the competitiveness of, existing insurance companies. As Tanega explains, ‘new insurers, unencumbered by a legacy of past liabilities, could underprice any firms seeking to pass on old liabilities’. 583

582 American Law Institute 1991, p. 80-86.
583 See Tanega 1996, p. 133.
The efficiency of liability insurance is also negatively affected by the problem of exclusive coverage. Tort-law systems often provide coverage that people do not purchase in a first-party context. This is the case, for instance, for pain and suffering, which are not, or only at very low, fixed sum levels, insured in first-party markets.\textsuperscript{584} Cane aptly notes that the fact that people do not normally purchase first-party coverage for non-pecuniary losses must raise doubts about the desirability of retaining damages for non-pecuniary loss in the tort system.\textsuperscript{585} The English public, Atiyah observes, does not yet understand that they themselves are paying for the damage awards. The erroneous perception that wrongdoers are paying ‘fuels demands for more and higher damages’.\textsuperscript{586} Once this misperception has been corrected, there is no ground for supposing that the public wants to pay for the coverage offered by the liability system.

It should be noted that the administrative cost (i.e, the cost associated with administering an insurance programme: reflecting the portion of the total amount that does not go to compensation for harm suffered) of first-party insurance and liability insurance differs significantly. Certainly, the administrative cost of liability insurance is much higher than the administrative cost of first-party insurance. As the authoritative American Law Institute concluded, ‘third-party tort insurance is extremely expensive to administer.’\textsuperscript{587} Priest reports that in the USA, the administrative cost of first-party plans are approximately 10\%, but for third-party, tort-law plans, they exceed 50\%.\textsuperscript{588} In the UK, the Pearson Royal Commission estimated that during the period 1971-1976 some £200 million a year was paid out in damage in tort claims at an administrative cost of £175 million. Thus, of every pound paid in liability insurance premiums about 53\% goes to pay damages and about 47\% goes to pay lawyers’ fees and other costs.\textsuperscript{589} Atiyah guesses that in 1997 something in the order of £2 billion was paid out in damages at a cost of a little under £1 billion in expenses.\textsuperscript{590}

Finally, it is relevant to note that liability insurance, unlike first-party insurance, has regressive income effects. Regressive income effects result from a lack of differentiation in the ‘insurance premium’ in the third-party context. The tort-law insurance premium, which is included in a product’s or service’s price, is the same for all consumers, although some, i.e. the high earners, bring higher risk (e.g. with respect to the size of potential loss of income) to the insurance pool than the low income earners, and, thus, purchase more coverage for the same price.

Substantively, in light of the analysis set forth above, the risk-spreading objectives of liability rules are unpersuasive to the extent that they rely on insurance. Where liability is aimed at risk spreading through insurance, the issue is whether the risk-reduction and risk-spreading functions discussed above should be pursued through third-party liability insurance or direct first-party insurance. A careful analysis of insurance mechanisms shows that the liability system is not an attractive way to spread risk, at least where liability is not justified on deterrence grounds.\textsuperscript{591} In many ways, first-party insurance is a more efficient and otherwise more attractive alternative than third-party liability insurance.\textsuperscript{592} As discussed above,

\textsuperscript{584} Priest 1992; Faure 2000, p. 107. For an argument that there is demand for insurance coverage for pain and suffering in a first-party context, see Croley and Hanson 1995, p. 1785.
\textsuperscript{585} See Cane 1999, p. 247.
\textsuperscript{586} See Atiyah 1997, p. 1113.
\textsuperscript{587} American Law Institute 1991, p. 30.
\textsuperscript{588} See Priest 1989, p. 38.
\textsuperscript{589} See Atiyah 1970, p. 125.
\textsuperscript{590} Ibid., at 153. See also Van Dam 1993.
\textsuperscript{591} Priest 1987; Priest 1991, p. 31-50. It has been argued that the deterrence incentives generated by liability in the real world (i.e. taking into account all other incentives and disincentives impacting an operator's decisions) are uncertain. See Bergkamp 2003, Chapter 5.
\textsuperscript{592} Priest 1987.
disadvantages of third-party liability insurance, as compared to first-party insurance, include the lack of effective control over adverse selection and moral hazard, problems of excessive and retroactively expanding coverage, regressive income effects, and the high administrative cost of this system. The problems of adverse selection and moral hazard become worse and more difficult to control when we move from fault to strict liability. In a first-party policy, premiums can be set in the function of the risk brought to the pool and the coverage offered; premiums for third-party liability insurance cannot be differentiated to the same extent and, accordingly, the price mechanism does not work optimally, as a result of which the total risk increases. Compensation systems other than liability typically offer a much lower level of recovery for non-pecuniary losses than those available in liability suits. Furthermore, victims may be in a better position than those causing the injury to diversify risk. Risk spreading may provide a justification for compensating and spreading losses, but it does not justify doing so through a liability rule.

6.1.4. Conclusions Insurance Theory

One of the main conclusions is that insurance can perform its useful risk-aggregation and risk-reducing functions only if the risks to be insured are sufficiently probabilistic and predictable, as well as statistically independent. Uncertainty as to the scope and size of liability seriously undermines insurability of liability risks.

In terms of first-party insurance versus liability insurance, in general, first-party insurance provides a much better ability to control the major threats to insurability, i.e. adverse selection and moral hazard. In other words, in terms of insurance efficiency, first-party insurance is superior to liability insurance.

There are issues around the insurability of catastrophic risk. The analysis showed, first, that liability for widespread damage, unlike, for instance, product liability for personal injury caused by defective goods, does not necessarily spread risk, and insurance does not function adequately in this context and does not produce risk-aggregation and risk-reduction benefits, unless it operates at very large scale. Significant uncertainty as to the scope and size of potential liability exposure undermines insurability. If no reliable assessment of the monetary size of the potential liability exposure is possible, insurers cannot accurately predict risk. Monetary and time limits on potential liability exposure, generally, enhance insurability.

As discussed above, insurance works only if risks are insurable. Whether the risks of terrorism are insurable, is discussed below. We discuss first how insurance, given that risks are insurable, manages risks. As noted above, insurers have to manage two types of risks:

593 As Bishop points out, this problem is addressed in several ways: “First, liability is often narrowly defined ... Second, liability is subject to Limitation on recovery. Third, it has been suggested that courts ought to adopt a defense of ‘extra-sensitivity’ of the plaintiff ... Fourth, where tort rules are used in a consensual setting (for example, product liability cases) ... , duty to warn doctrines are concerned with the information transfer problem’. See Bishop 1983, p. 241-266.

594 Epstein 1985, p. 645-669. Epstein has commented that ‘it is difficult to estimate the total loss wrought by incorrect design of the products liability system’; ibid, at p. 668. See also Snijders 1993, p. 2-6. Shavell has argued that regulation of liability coverage, requiring or forbidding insurance, may improve diluted incentives arising from judgment-proof problems or improve the possibility of escaping from liability when insurers are able to monitor insured behaviour. It. remains unclear however how this ability should be assessed and whether government intervention in the insurance market should be preferred over the market in any situation. See Shavell 2000. Noting that it is much more expensive to insure victims through the legal system than directly by first-party insurance coverage, Shavell rejects the typical justification for mandatory liability coverage where it provides an implicit form of insurance protection for victims.

595 See Cane 1999, p. 405.

adverse selection and moral hazard. At the level of individual contracts, the focus is on managing the risks associated with moral hazard. In addition, insurers can manage their overall risk exposure generally through mechanisms such as pooling, reinsurance, etc., which is not discussed further because it is not relevant for purposes of this study. The same is true for risk management through ‘claims-made’ versus ‘loss occurrence’ policies, which again is not relevant to this study.

Insurers employ instruments such as deductibles, co-insurance, caps, exclusions, premium differentiation, bonus/malus mechanisms, and the like, for managing risks. These concepts can be defined as follows:

- **Deductibles**: also called ‘own risk,’ i.e., the amount that the insured must bear before insurance kicks in;
- **Co-insurance**: under this arrangement, the insurance policy covers only a portion (typically expressed in a percentage of less than 100%) of the damage, with the remainder being for the account of the insured;
- **Caps**: the upper financial limit of an insurance policy, i.e., the maximum amount that the insurer will pay out under the policy (per year, per event, or otherwise);
- **Exclusions**: these are specific events, types of damage, causes of damages, or other aspects, that are excluded from insurance coverage and thus for the insured’s account;
- **Premium differentiation**: charging different amounts of premiums to different insureds based on the nature and scope of insurance coverage provided and the risk that the insured brings to the risk pool;
- **Bonus/malus mechanisms**: such a scheme involves premium reductions for insureds with a good accident record (no or few claims) and premium increases for those with a bad record (many claims), and are intended to create incentives for damage- and claims-avoiding behaviour.

### 6.2. Industry practices within sectors exposed to analogous risks

In this section, we will analyze the use of contracts, general terms and conditions, and industry-wide concepts at various levels (regional, national, or European), such as shared risk pools, used as potential tools for managing third party liability risk. The following sectors of industry will be considered:

- Pharmaceutical industry;
- Software companies, in particular cyber security software companies; and
- Meteorological forecasters.

The practices of companies in these sectors are determined based on two methods: (1) desk research of publicly available sources, including public information in the area of public procurement; and (2) information requested from selected trade associations active in the sectors of industry covered.

In terms of structure, the practices for each sector of industry are analyzed and presented in accordance with a fixed outline framework, as follows:

- **Nature of Potential Risk Exposure** (including damages, scope, historical exposure)

---

597 A bonus/malus scheme involves premium reductions for insureds with a good accident record (no or few claims) and premium increases for those with a bad record (many claims).


599 This corresponds to Tasks 4.1 and 4.2 of Work Package 4.
Current Industry Practices to Limit Exposure Contractually (liability limitation used in contracts/risk sharing and mutualisation pools/liability capping and exclusion schemes, availability, prevalence and nature of insurance contracts used)

Following an overview for each of the covered sectors of industry, we present an assessment of the effectiveness of these mechanisms in potentially reducing exposure to third party liability in the security industry. This part focuses on the question as to which of the mechanisms identified could effectively reduce security providers’ liability exposure. To answer this question, the basic structure of the security industry will be compared with the basic structure of the other covered industries.

Before going into the discussion of the limitation mechanisms utilized in each of the covered industries, we provide below a brief introduction to the industries concerned, and their liability exposure.

The covered sectors of industry are exposed to potentially major liability exposure for damages such as property damage, personal injury, including medical expenses and disability, pain and suffering (‘moral damage’), environmental damage, and economic losses (lost profits). In theory, each of the sectors of industry could be exposed to claims for each of these types of damage. Unsafe, defective, or ineffective pharmaceutical products could result in many cases of personal injury, which could lead to medical expenses, loss of income, pain and suffering, etc. Defective or ineffective software, for instance, security software, could result in unavailability of e-commerce websites, resulting in massive loss of income, or as gateways to the ‘hacking’ of computer systems for managing critical infrastructure, such as nuclear power plants, which could cause a nuclear accident with many casualties, massive property damage, environmental contamination, and enormous loss of income. Likewise, incorrect meteorological reports could cause trouble for airplanes, ships, or cars, and result in accidents, with associated personal injury, property damage, medical expenses, and loss of income. Thus, in terms of the potential for exposure to massive liabilities, the pharmaceutical, software, and meteorological industry may be in a position similar to the security industry.

There may be large differences, however, in terms of probability of the risks of actual incidents and of the risks of incurring liability therefor.

With respect to accidents leading to potential liability exposure, the level of regulation of a sector of industry may play a role. Of the covered sectors, the pharmaceutical industry is heavily regulated; the other sectors are regulated to a lesser extent. The level of regulation of the security industry would appear to be somewhere between the pharmaceutical industry and the other sectors. The level of regulation may have an influence on liability exposure. Extensive regulation does not necessarily imply reduced liability exposure; regulation, of course, may have this effect if it is effective in reducing the actual risk of accidents. Conversely, it is also conceivable that onerous regulatory standards could result in increased exposure, where plaintiffs can invoke non-compliance in support of claims based on negligence.

The level of regulation is probably not a main factor when it comes to terrorism risk. The actual risk of terrorism is a function of many variables, such as the political situation, the attractiveness of a target, the level of protection at the target, the sophistication and specialization of the terrorists, etc. If, in deciding where and when to attack, terrorist do some sort form of cost/benefit analysis, their decisions may be predictable. Experience has shown that attacks targeting means of transportation (airlines, subways, etc.) are fairly common, often in large metropolitan centers (e.g. capital cities). Cyber-attacks, on the other hand, do not appear to have been frequent, or if so, are at least not typically successful. The actual risk levels between various sectors of industry therefore may differ substantially.

Whether companies in a particular industry sector are able to impose contractual liability limitations and indemnification obligations on their customers is a function of the structure of
the market, the main types of customers, their bargaining power, customs, and other factors. There may be substantial differences between sectors of industry in this regard. For instance, small companies may be more inclined willing to accept large liability exposure, large public entities may be in a position to reject any liability limitation, etc. The law may also restrict the use of liability limitations; for instance, under the Unfair Contract Terms Directive blanket liability limitations which unfairly bias contracts against consumers are not allowed. These factors, however, cannot be explored in detail in this report. In the assessment of the contractual limitation mechanisms, however, some observations on these issues will be made.

6.2.1. The software industry

The ‘software’ industry is not easily defined. Within its scope lie a myriad of specifically designed software applications to deal with tasks ranging from word processing to astrology. Moreover the term also encompasses system software, i.e. the inter-dependent layers of programs which govern the basic functionality of electronic products such as computers, as well as the range of computer programming tools which allow further programs to be developed, tested, and manipulated.

Within that range of functions there of course lies that application software which is specifically designed for cyber-security purposes, i.e. the protection of information and network integrity from malicious agents, be they generic viruses, malware, specific hacking attempts etc. Such software is typically used on individual computer devices or terminals rather than for the protection of Industrial Control Systems, for example. However, to the extent that security software on an individual computer may be the access point or target for an attack on a security network, discussion of software in the context of critical infrastructure or other security networks is at least potentially peripherally relevant and will to this extent inform our analysis here.

For ease of reference in the discussion that follows, ‘software’ and the ‘software industry’ will be dealt with under its colloquial understanding as referring only to ‘application software’ i.e. programs which are designed and marketed independently for a particular purpose or task, readily separable from the basic functioning systems which run computers otherwise. Examples include identity and password managers, content management systems, animation and graphics programs, data management software, cyber security software, etc.

Application software is deliverable in two ways (i) packaged, via a real and deliverable medium such as a disc or box, (ii) ‘as a service’ i.e. leased from a provider for installation/download.

6.2.1.1. Nature of potential risk exposure

The types of damages that the software industry is facing will vary depending on the nature of the program offered. Among the most pertinent, however, are those offered by data-management and cyber security programs. Providers of these programs in particular could potentially be exposed to claims based on data loss, property damage, economic losses, consequential/incidental loss derived from the loss/misuse of data, product liability claims, and breach of contract.

600 Industrial Control Systems are command and control networks and systems which support industrial processes. They are responsible for the monitoring and controlling of processes and operations often within critical infrastructure and services including electricity distribution, water treatment, oil refining, railway transportation, etc. See European Network and Information security Agency 2011, p. 1.
Such claims for damages may arise in the context of unintended malfunctions or omissions resulting, for example, in data losses through a lapse in security software, or from a directed attack on an individual or group of individuals’ data which security software (e.g. anti-virus/malware software) is incapable of fending off).

As with the security industry, incidents of cybersecurity breaches affecting users are broadly on the increase, and with them disruption to computer functionality and thus the supply of computer-based services. Indeed, like the security industry the provisions of programs for data management and cyber security are increasingly vulnerable to attack or incursion from terrorist or maleficient actors, a threat which is evolving at a pace similar to the ever dynamic nature of the terrorist threat to the security industry, such that the software industry is constantly having to modernize and evolve to resist it. Furthermore, in respect of data management software, a malfunction could lead to the loss of huge amounts of valuable data and all the attendant consequential losses which could be associated with it.

As with the security industry, the nature of the cyber-terrorist or hacker threat posed to the industry by security incidents is international in aspect and character. Given such attacks/incidents often operate across international borders there are, of course, difference legal frameworks and jurisdictions involved. Further similarities can be pointed to in the extent to which the industry must necessarily rely on Member States security forces to track and apprehend offenders, not being in a position to undertake such actions and thus mitigate this aspect of an incident’s likelihood themselves.

Distinctive features related to the nature of the software industry and its products include the manner in which products are delivered, the pace at which threats and indeed products themselves evolve, and the role of the end user in exercising caution and deploying cyber security software themselves to ensure the integrity of their information. For all the types of software outlined, the majority of customers fall into the categories of private end users/customers, and business customers utilising software for whole firms and/or business purposes. At the point at which a license agreement is concluded and executed, bargaining power invariably rests with the software provider with agreements frequently stipulating that unless the pre-drafted license agreement is accepted by the customer no sale will go ahead. For example, agreements will frequently depend on qualifying clauses such as “if you do not agree to these terms do not access or use the software”. With downloadable software, the user’s ability to install or download the product will not be realized without acquiescing to the terms by clicking on an ‘I Agree’ option at the outset of installation/download.

There is no specific EU regulation dealing directly with the liability or liability exposure of the software industry. However, there is some potential cross-over with existing regimes which deal with the regulation of product and service providers:

- Relationship with the Services Directive

The Services Directive directly governs the relationship between a service provider and customer. It is likely the case, however, that the provision of software packages that are sold ‘as is’ to end users, do not meet the definition of ‘service’ under the Services Directive, which

601 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ‘Cyber Strategy of the European Union: An Open, Safe and Secure Cyberspace’ JOIN (2013) 1 final, 3.
602 Id., p. 17.
holds that ‘service’ means “any self-employed economic activity, normally provided for remuneration, as referred to in Article 50 of the Treaty.”

The reference here to an ‘activity’ would likely preclude software programs. The provision of high-end tailored security services with the involvement of security software firms could potentially fall within the definition, but to the extent that this crosses the boundary between software and security-service provider it is noted that the security industry is specifically precluded from the Directive’s scope and would thus not be of application to such actors.

- Relationship with the Product Liability Directive

The Product Liability Directive establishes a system of unlimited liability in the case of a product defect, or the act or omission of a third party. The definitions of ‘product’ and ‘producer’ under the Directive, however, likely exclude cyber security and other deliverable application software products.

According to Article 2 ‘product’ means “all movables even if incorporated into another movable or into an immovable. ‘Product’ includes electricity”. ‘Producer’ means “the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer” (Article 3 (1)).

Nevertheless, it is conceivable that pre-packaged, deliverable software could potentially be considered to fall within its scope.

Relationship with Data Protection Legislation

The Data Protection regime in the EU is covered by a host of legislative and policy measures. Directive 1995/46 EC is the base instrument, although it is due to be replaced with proposals currently in place for a new Data Protection regulation in 2013. Although the Data Protection regime is centred on the protection of personal data from unauthorized sharing, selling, holding etc, it is of some consequence to the software industry. Under Article 17 of the 1995 Directive, Member States transposing legislation must require that personal data controllers implement appropriate technical measures to protect the data which they hold against destruction, loss, alteration and unauthorized disclosure and access. Thus it is clearly the case that cyber-security measures must be put in place which may include cyber security software applications, password protectors, data management applications, etc.

Moreover, Article 17 stipulates that controllers may have regard to the state of the art and the cost of the implementation of such measures. This signals, that in the case of data management and security at least, it is not necessary to employ impenetrable security

604 Article 4 (1).
605 Article 2(2)(k); note that an exemption also applies under Article 2(2)(i) to “activities which are connected with the exercise of official authority…”, which could potentially be understood to cover providers working as subcontractors for exercisers of such authority, at least where there is no fault.
607 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
608 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection regulation) COM (2012) 11 final; the security measures under Article 17 of the 1995/46/EC Directive can be found under Article 27 of the proposal.
measures irrespective of the available technology or the cost of such measures, which may be of consequence as a defence to negligence claims in such contexts.

Relationship with EU Cyber-security Strategy

Cyber-terrorism, cyber-crime and cyber-security are all becoming an increasing concern within the European Community and the EU is about to agree on a Directive on attacks against information systems, especially through the use of botnets. Along with that Directive it has also developed a strategy which will establish common minimum requirements for Network and Information Sharing (NIS) which will see Member States designate competent national authorities on the security of network and information sharing systems, set up computer emergency response teams, and adopt national strategies and cooperation plans.609

With respect to the relevance of this strategy and proposed legislation to the software industry, those companies which are also involved with the provision of security to critical infrastructure (although not strictly speaking ‘software companies’) will most likely see the rise of good practice guidelines from Member States in coming months as Member States, as part of the Cybercrime Strategy, have been invited to use the purchasing power afforded them in public administration, such as via public procurement, to enhance good practice standards and encourage the development of cyber security practices and policies.610 Member States are further invited thereunder to improve the preparedness and engagement of the private sector and encourage the industry to build its own cyber resilience capacities and share best practices across sectors. Further areas of relevance could refer to the extent to which the strategy intends to make the internet ‘safer’ and foster cooperation on dealing effectively with cyber threats.

6.2.1.2. Current industry practices to limit exposure contractually

Limitation of primary obligations and disclosures and warnings

The primary method employed by the software industry to limit its third party liability is through the use of liability exoneration clauses in its end user license agreements for application products. These are employed comprehensively across the markets for both packaged programs and those which are sold without the use of a ‘real’ medium. Because software programs in these formats are not ‘products’ in the conventional sense, they are governed by lease agreements with users which provides them with access to the copyrighted program. These leases will either be perpetual (or for such a duration of time as to make them practically so) or will be for a set period of time, whereupon the user will have to pay a fee to upgrade the software and use the new model. This model of trade means that the contract governing transactions is an end-user license agreement (EULA) rather than a contract of sale.

EULAs take two dominant forms in the sale of application software: (i) for those which are packaged, agreements commonly referred to as ‘shrink wrap’ licenses take the form of a EULA enclosed, but readable, through the packaging, based on the understanding that opening the ‘shrink wrap’ will constitute an agreement to the terms contained therein; (ii) increasingly replacing them, and commonly utilized for downloadable software programs, ‘clickwrap’ agreements or licenses (also known as ‘click through’ agreements or licenses) are those EULAs presented to prospective users at the outset of a download/upload of software

609 Id., p. 5.
610 Id., p. 6.
programs or packages which will not allow the transaction to proceed until the user acquiesces to the terms, usually by clicking upon an ‘I Agree’-style tab or equivalent.

Clickwrap agreements, as well as specifying the terms and conditions of use, invariably contain liability limiting/exoneration clauses. For example, one cyber-security software company’s agreement for the 2006 version of an antivirus product, under a clause titled ‘Disclaimer on Damages’ reads:

“TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL [the company] OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.”

Shrink wrap agreements contain similar exclusions. For example, another software company’s Terms of Use under a Licensing Agreement for office software, under ‘Limitation on and Exclusion of Damages’ reads:

“YOU CAN RECOVER FROM [the Software Company] AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO THE AMOUNT YOU PAID FOR THE SOFTWARE. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to
· anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
· claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if
· repair, replacement or a refund for the software does not fully compensate you for any losses; or
· [The software company] knew or should have known about the possibility of the damages.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.”

The extent of the limitation will depend on the particular license agreement, but some will attempt to restrict a user’s attempt to apply for any damages whatsoever, even beyond the liability cap specified.

Liability caps

Liability caps are also built into EULA agreements, although their upper limit varies by nature of the program offered and by provider. Many are restricted to the purchase price of the EULA, some to a nominal amount. One company’s License Agreement for basic computing software packages, for example, reads as follows:

“Circumstances may arise where, because of a default on [the company]'s part or other liability, Licensee is entitled to recover damages from [the company]. Regardless of the basis on which Licensee is entitled to claim damages from [the company] (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), [the company]'s entire liability for all claims in the aggregate arising from or related to each Program or otherwise arising under this Agreement will not exceed the amount of any 1) damages for bodily injury (including death) and damage to real property and tangible personal property and 2) other
actual direct damages up to the charges (if the Program is subject to fixed term charges, up to
twelve months' charges) Licensee paid for the Program that is the subject of the claim.”
This limit also applies to any of [the company]'s Program developers and suppliers. It is the
maximum for which [the company] and its Program developers and suppliers are collectively
responsible.

Just as prevalent, however, are more stringent liability cap clauses. As another example,
another prominent cyber security software provider’s EULA, under Clause 6 ‘Limitation of
Remedies and Damages’, reads as follows:

“Regardless of whether the claim for such damages is based in contract, tort and/or any other
legal theory, in no event shall either party’s aggregate liability to the other party for direct
damages exceed the lesser of:
a) the amount of total fees paid or payable by you for the Software giving rise to such claim
during the 12 months immediately preceding the event giving rise to such claim, or
b) the applicable […] list price, at the date of the purchase, for the Software giving rise to
such claim ordered by you during the 12 months immediately preceding the event giving rise
to such claim,
even if the other party has been advised of the possibility of such damages.”

Indemnification

EULAs will sometimes indemnify providers even against providing basic functionality and
security. Not all will do so, however, although where basic functionality is warranted it is
almost always limited in time to a period of one or two months, typically. Customers with
products which are warranted in this manner will usually only be entitled to repair,
replacement, or refund of the purchase price.

For example, see one company’s License Agreement on Warranties:
a. General. [the company] warrants that, on delivery of the Software and for a period of thirty
(30) days thereafter, that (i) the medium (if any) on which the Software is delivered will be
free of material defects, and (ii) subject to Section 6(c), that the Software will perform
substantially in accordance with the applicable specifications. The foregoing warranty applies
only to the Software as originally delivered, and does not apply to Updates. Your sole and
exclusive remedy for breach of this Warranty is replacement of the defective media or
Software or, at [the company]'s option, return of the Software for a full refund. In order to
exercise your rights under this Section 6, you must uninstall and destroy all copies of the
Software you may have made (including all archival copies), and (i) if you purchased the
Software by download, follow the instructions [on the company website] and contact us with
your refund request, or (ii) for all other purchases, return the Software in its original package,
along with your receipt, to the point of purchase.

b. Free Software and Services. THE PROVISIONS OF THIS SECTION 6.b APPLY IN
PLACE OF SECTION 6.a WITH RESPECT TO FREE SOFTWARE AND […]FREE
SERVICES. ALL FREE SOFTWARE AND […] SERVICES ARE PROVIDED ON AN “AS
IS”, “AS AVAILABLE” BASIS, WITHOUT WARRANTY AND WITHOUT SUPPORT OR
OTHER SERVICES BY [the company]. THE FOREGOING ALSO EXPLICITLY
APPLIES FOR [the company’s] ANTI-VIRUS [particular] EDITION FOR [a particular
operating system].

c. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED BY SECTION 6.a OF THIS
AGREEMENT, [the company] DISCLAIMS ALL OTHER WARRANTIES WITH
RESPECT TO THE SOFTWARE AND/OR SERVICES, MEDIA AND ANY OTHER
SUBJECT MATTER OF THIS AGREEMENT, WHETHER EXPRESS OR IMPLIED,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF
MERCHANTABILITY, THE IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND IMPLIED WARRANTY OF NONINFRINGEMENT. [The software company] DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE AND/OR SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, THAT THE SOFTWARE WILL PROVIDE 100% PROTECTION OR THE INTEGRITY OF SELECTED DATA, INFORMATION OR CONTENT STORED OR TRANSMITTED VIA THE INTERNET. Some jurisdictions do not allow limitations on certain implied warranties, so the above limitations may not apply to you. You may have other rights that vary from jurisdiction to jurisdiction.

d. Hazardous Environments. You acknowledge that the Software is not designed or licensed for use in hazardous environments, including without limitation operation of nuclear facilities, aircraft navigation systems, aircraft communication systems, air traffic control, life support or weapons systems and any other environment in which bodily injury or death could result from failure of or inability to use the Software. Without limiting the provisions of Sections 6.b and 6.c of this Agreement, [the Software Company] and its licensors hereby disclaim any express or implied warranties of fitness for such uses.

As well as exclusion from statutory and implied warranties, see also on Indemnification: You agree to indemnify, defend and hold harmless [the company], its Affiliates and their respective directors, officers, employees and agents, licensors, representatives from and against all losses, expenses, damages and costs, including reasonable attorneys' fees, resulting from your use of the Services or any violation of this Agreement by you, including but not limited to any breach or alleged breach of any of your representations, warranties or undertakings hereunder. [The company] reserves the right to assume, at its sole expense, the exclusive defense and control of any matter subject to indemnification by you, in which event you will fully cooperate with [the company] in asserting any available defenses.

Exclusions (force majeure etc.)

Exclusions will apply (see above) where the use of the product does not comply with the terms of use specified in the EULA. Any use outside the terms of service will negate any warranty and the EULA itself. Terms will vary by product and provider but tend to cover such areas as limitations to private use only, use that does not involve the handling, production, storage, viewing or enjoyment of copyrighted material, use on a single computer/device only, prohibitions against lease/lending/sub-licensing/making copies for distribution/any of the aforementioned, prohibitions against manipulating/reverse-engineering programs, etc.

Insurance

Although orthodox business insurance will typically cover third party liability it will almost invariably only cover ‘tangible’ assets, which will typically exclude electronic data. To specifically deal with electronic data related losses, the insurance industry does offer cyber liability insurance.

As well as being increasingly common to protect against first-party losses as the result of a cyber security breach, cyber liability insurance can also be used in respect of third party losses. Policies are available which will cover liability and defense costs for claims arising out of any security breach including identity theft, negligence, computer theft, extortion deriving from a network/data breach, or any unintentional act, mistake, error or omission by an employee resulting in a breach. Coverage is also available to cover the costs of transmission of computer viruses and denial of service attacks and will cover civil suits and the payment of civil fines and penalties.
For software companies specifically offering privacy protection as part of their product portfolio, privacy liability policies are also offered by the insurance industry covering direct, contractual, and third party liability. Premiums for software providers are calculated based on their exposure and are generally capped. Both the cap and the premium will be commensurate to the company size, risk exposure, the type of data stored/protected (e.g. medical records, personal or financial data, and sensitive business information will attract a higher premium), size of the customer base, etc.

Mutual risks pools or similar arrangements are not common in the software industry. A recent study did not find any mutual risk pools operating in the software industry.611

6.2.2. The pharmaceutical industry

The ‘pharmaceutical industry’ can be broadly defined as that associated with the development, patenting, and sale of pharmaceutical products. Pharmaceutical products are included within the conception of ‘medicinal products’ within the EU, as defined by the Medicinal products Directive as “any substance or combination of substances presented for treating or preventing diseases in human beings. Any substances or combination of substances which may be administered to human beings with a view to making a medical diagnosis or restoring, correcting or modifying physiological functions in human beings is likewise considered a medicinal product.”612

Within the auspices of ‘medicinal product’ a ‘proprietary medicinal product’ is further distinguished as encompassing “[a]ny ready-prepared medicinal product placed on the market under a special name and in a special pack.”613

It is the industry involved in the development, marketing, and sale of such drugs which is meant here by reference to the ‘pharmaceutical industry’.

6.2.2.1. Nature of potential risk exposure

The primary liability risk to which pharmaceutical companies is exposed is that derived from product liability, as covered by the Product Liability Directive.614 Product liability actions for damages may be brought under negligence, warranty and strict liability situations. In terms of the application of strict liability for product defect, manufacturing defect, design defects and ‘failure to warn’ may be all invoked.

The scope of the potential damage is substantial if one considers, for example, the extent of the thalidomide disaster in the 1950’s which resulted in the malformation of over 12,000 infants after their mothers’ ingestion of the drug during pregnancy. Accumulated damages to three generations of sufferers have thus far numbered into hundreds of millions of euros in compensation, with cases still ongoing.

611 Ernst and Young, ‘Study on co(re)insurance pool and on ad-hoc co(re)insurance agreements on the subscription market’ COM (2013).
613 Id., Article 2

197
The scope is somewhat limited, however, by the nature of the industry. Manufacturing defects are minimized by strictly controlled manufacturing standards. Design defects are similarly minimized in so far as all new drugs are subjected to approval either by the relevant Member State or through the European Medicines Agency’s (EMA) quality, safety, and efficacy testing before authorization to enter the market will be granted. Once placed on the market drugs also continue to be monitored for defects through the pharmacovigilance monitoring procedures operated by the EMA and Member State regulatory authorities, as well as widespread pharmacovigilance processes operated within and by the industry itself.

Pharmaceutical products fall within the scope of the Product Liability Directive which creates an unlimited liability regime for manufacturers of defective products.\textsuperscript{615}

The Directive, however, does allow for what has come to be known as the ‘development risks defense’ under Article 7(e) which may be relevant to pharmaceutical producers. It provides that ‘[t]he producer shall not be liable as a result of this Directive if he proves(…) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be known’.

This would, for example, have relevance to side-effects which for which testing methods did not exist previously. Under Article 15(1), however, Member states are empowered to implement regimes which, by way of derogation from Article 7(e), will allow producers to be found liable even where they can demonstrate that the state of scientific knowledge at the time was not such as would have allowed the defect to be defective. This is a discretionary power which Germany has elected to implement for pharmaceutical products, and which Luxembourg and Finland have completely disallowed for all products.\textsuperscript{616}

The organization, marketing and distribution of products to pharmaceutical companies’ customers is rather a unique process. First of all, drugs are generally selected by doctors or clinicians for their patients; patients themselves have very little to do with the selection of one particular brand of drug over another analogous competitor. Moreover, the consumer does not bear the full cost burden of the product. Depending on the Member State in question health insurance, social healthcare and government subsidies for pharmaceutical purchases on prescription all impact the extent to which the end-user will bear the cost of the product to the extent that purchasing power is concentrated in the hands of those other actors rather than the patient who uses it.

Moreover, drugs are not bought directly from companies but rather are routed through pharmacies as well as hospitals, clinics and health institutions acting as dispensaries. The extent thus that a company will be in a powerful bargaining position with respect to physicians prescribing their drug will depend on their network of sales associates and dominance in the market place, and, the nature of the drug involved. If the particular drug is still under patent then only the patent-owning company will be in a position to supply it, a particularly powerful position where like products are not available. After the expiry of the parent, however, the bargaining power of companies is weakened as the drug can be manufactured by its competitors, creating competition for customers within the market.

\textsuperscript{615} See section 3.2.5 of this report.

\textsuperscript{616} Spain has also excluded the defense for pharmaceutical and food products, and France for products derived from human body parts such as blood products.
6.2.2.2. Current industry practices to limit exposure

Under Article 12 of the Products Liability Directive it is not possible to disbar liability claims for personal injury from products covered by its auspices. It reads: “The liability of the producer arising from the Directive may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability”.

However, there are certain provisions which may limit the extent of that liability. One is the development risks defense under Article 7(e).

Limitations of the extent of companies’ liability exposure may also arise in the context of cases involving the contributory negligence of the patient, as provided for under Article 8(2).

Where products are used in a manner inconsistent with instructions and warnings, or for uses for which they are not intended, exclusions will also apply. There is, however, potentially some scope for the suggestion that in situations where a manufacturing pharmaceutical company was aware or ought to have been aware, that its product was likely to be used to treat a class of ailment for which it was not marketed, that company could conceivably be held liable for damages caused under the provisions of Article 6(2) which holds that products will be held to be defective where they do not provide the safety standard a user is entitled to expect, taking into account “(b) the use to which it could reasonably be expected that the product would be put”.

No limitation of liability is allowed under the Directive, although in the specific circumstances of class-actions style suits where death or personal injury is caused by identical defects in identical product items Member States may provide that a producer’s total liability in each case may be limited to an amount not less than €70 million.

Liability can be shared, however, and the industry has included this in certain contractual arrangements with Member States particular in the case of vaccine and anti-viral drugs. In this case particularly, the pharmaceutical industry is, however, in a much strengthened position due to the nature of the products in question. This asymmetry of power, both between the pharmaceutical industry and prospective customers at times of scarcity of supply, is highlighted by the case of the vaccine crisis of the H1N1 outbreak in 2009. Declared a pandemic on 11 June 2009, the announcement precipitated something of a scramble by Member States to procure vaccines, particularly for ‘high risk’ groups upon whom the virus was having more severe effects, including death. Vaccines thus had to be speedily purchased, acquired, approved and in some cases developed to feed this demand. Most were approved through normal procedure (e.g. Pandremix, Focetria, Celvepan), although there have been suggestions that some were approved nationally through a somewhat expedited procedure, perhaps indicative of how concerned certain Member States were about procuring vaccines quickly.

The activation of ‘sleeping contracts’ between major pharmaceutical firms, as well as companies wishing to honor loyalties with particular Member States, meant that some

---

617 Although, as discussed above, it is open to Member States to deny respondents recourse to that defense through stricter national measures under Article 15.
620 Some Member States had initiated ‘sleeper contracts’ for influenza vaccines with pharmaceutical companies after the Avian Flu outbreak 2006-2007, which were to be ‘activated’ upon the declaration of an influenza pandemic by the World Health Organization.
Member States were very much disadvantaged in the acquiring of such vaccines, particularly those who had no emergency plans for such eventualities in place. It is commonplace in the industry that when it comes to the roll-out of vaccine programmes by Member States, particularly with high risk groups, that the pharmaceutical industry will limit its civil liability in such cases by contracts with the Member State involved, such that liability will be shared. However, in this instance certain Member States had to accept increased liability, due to the shortage of supply and asymmetry of bargaining power.621

In part in response to the liability issue, but also to ensure supply in future situations, the European Commission issued a proposal on future dealings with serious health threats with a transboundary aspect in the future.622 The measure proposes the provision of a legal basis for an EU mechanism for the joint procurement of medical countermeasures in which contracting parties could participate on a voluntary basis in order to purchase medical countermeasures, such as pandemic influenza vaccines, thereby improving preparedness for future pandemics. The proposal would see a common contractual position amongst all contracting parties negotiated, which would include a common understanding on liability issues i.e. the extent to which Member States would be willing to share liability for side effects with vaccine manufacturers, so as to avoid the kinds of variances in contractual obligations which characterised the H1N1 situation.623 Member States would take part on a voluntary basis, and still retain autonomy in respect of their response plans and preparedness.

The proposal is currently before the Council which intends to undertake further discussions with the aim of enabling the Irish Presidency to engage in negotiations with the European Parliament and move towards a first reading agreement.624

Mechanisms employed by the industry:

Mandatory Insurance Schemes

Under the strict liability regime created under the German Drug Act 1976, mandatory insurance is required of any person placing an authorised drug on the German market. Pharmaceutical companies are required to ensure that they can meet their compensation commitments as per the maximum exposure thresholds under the Act. They can do this by means of third party liability insurance, or an exemption or warranty guarantee issued by a bank/credit institution certifying that they are sufficiently capitalized to meet such requirements.

Liability is capped per person, per drug at €600,000 or €120 million for accumulated damages across several plaintiffs from the same drug.

In complying with the scheme certain companies can avail of a reinsurance pool in the ‘Pharma-Rücksversicherungsgemeinschaft’ (‘Pharma Reinsurance Group’).625 The pool covers precisely that product liability for all pharmaceutical products sold in Germany that the German Drug Act creates. Membership of the pool requires sufficient financial strength, i.e.

621 In the case of Belgium, see P O’Donnell, Minister admit flu errors: Call for joint strategy for dealing with drug firms, European Voice, 8 July 2010.
623 Id, p. 40.
625 Ernst and Young, ‘Study on co(re)insurance pool and on ad-hoc co(re)insurance agreements on the subscription market’ COM (2013), p. 391.
credit rating, establishment in a certain Member State, willingness to accede to the contractual
terms as prescribed by the pool, and the payment of pool premiums. 626

Voluntary Compensation Schemes

In the wake of the thalidomide tragedy, pharmaceutical companies operating in Sweden
collaborated with the Swedish government and insurance industry in establishing a voluntary
national compensation scheme. The scheme is funded by voluntary contributions from
pharmaceutical companies based on their total sales turnover in the Swedish market. It is
operated by the Swedish pharmaceutical insurance association, which also administers a
claims board in the form of an injury panel, to hear disputed claims for referral. Liability is
capped at SEK 10 million per person injured, and/or SEK 200 million for all injuries in a
given year. Liability is not strict but is determined on the basis of whether the person would
reasonably have absorbed the risks/side-effects suffered in light of the severity of their
condition. Negligence need not be demonstrated, however.

Although not a compensation scheme, further examples of voluntary collaborations within the
industry can be found in the form of the Finnish Pharmaceutical Insurance Pool, created by
the pharmaceutical industry to create its own compensation fund to cover its liabilities,
replacing the previous system where companies had been purchasing their insurance from
external insurers who had then been pooling the risks themselves. 627

Insurance

The pharmaceutical industry can avail of insurance cover and will invariably do so although
policies are capped in respect of litigation cover and third party liability due to the scope of
the damage possible.

6.2.3. The meteorological industry

Weather forecasting can broadly be divided into two particular types of service or product.
First there is the general provision of short-term forecasts to television channels, emergency
services, coastguards, etc., often also made available to the public at large. Such services are
conducted by both state-owned and private agencies. Secondly, there is the more bespoke,
tailored forecasting services offered to particular customers which are tailored (for example,
geographically or focusing on a particular weather aspect such as likelihood of snow) for
customers such as gritters, insurance agencies, airports, etc. This second subsector of the
industry is again carried out by both public and private agencies, under contract.

6.2.3.1. Nature of potential risk exposure

Depending on how liability is applied, in situations where forecasters provide negligently
inaccurate information, and such information is relied upon to tragic consequences, it might
be the case that they could be exposed to liability for death and personal injury, economic and
structural damages, and damages for pain and suffering, depending on the applicable Member
State rules. Damages for breach of contract may also be relevant.

Were it established that the forecaster could be held liable under negligence or breach of
contract rules, the scope of damage could potentially extend to any damage which could have

626 Id.
627 Id., p. 72.
been prevented had adequate warnings of a particular weather pattern been received or, conversely, any damages caused by negligent reporting of a likely weather event which led to damages accruing through evasive/evacuation efforts which were unnecessary.

There is no specific EU regulation dealing with the liability of weather forecasters, or standards of weather forecasting.

The average user of a weather service or a weather service’s website cannot generally be termed a ‘customer’ as the information provided is free of charge. To this extent such customers have very little bargaining power, and indeed access to such information (such as an on a national weather service website) is almost invariably provided according to a liability-limiting disclaimer stipulating that no responsibility is borne by the weather information generator for any damages caused by any reliance on any of the information presented.

The other main type of customer that weather forecasters have are particular companies, groups or industries who rely particularly on tailored weather information. Such relationships are formed under contract for the performance of specific duties by the weather forecasting services. The extent of such bargaining power will vary by industry and Member State. For example, gritters are not in as strong a bargaining position as national television channels, which may singularly constitute a forecasting agency’s largest source of income.

6.2.3.2. Current industry practices to limit exposure

Limitation of primary obligations and disclosures and warnings

Like the software industry, the meteorological industry is in a particularly powerful position insofar as the manner in which it relates to general end-users of weather information with whom it has no particular contract. In such circumstances access to that information, e.g. through a national weather service website, is made conditional upon disclaimers which and liability-limiting clauses.

The terms of use of one Member State’s national weather agency, for example, reads as follows:

Disclaimer

The services provided as part of the Site are experimental and have not been tested or verified. The [forecasting agency] does not consider any Content on the site to be representative of its weather information. You should not make any weather-related decisions based on the Content of this Site. To the fullest extent permitted by applicable law, the [weather forecasting agency] excludes all warranties and representations (express or implied) in respect of the content.

Your use of the Content is entirely at your own risk. We make no warranty, representation or guarantee that the Content is error free of fit for your intended use.

Limitation of Liability

to the fullest extent permitted by applicable law the [forecasting agency] hereby disclaims any and all liability for loss, injury or damage (direct, indirect, consequential, incidental or special) arising out of or in connection with use of the site including without limitation any and all liability: relating to the accuracy, completeness, reliability, availability, suitability, quality, ownership, non-infringement, operation, merchantability and fitness for purpose of the content; relating to its work procuring, compiling, interpreting, editing, reporting and publishing the content; relating to any interruption, failure or cessation of operation or transmission
resulting from any acts or omissions of any third parties in connection with your use of the site; resulting from reliance upon, operation of, use or actions or decisions made on the basis of, any facts, opinions, ideas, instructions, methods, or procedures set out on this site; arising out of or relating to the misuse of or inappropriate reliance on the content of the site; and resulting from any virus, worm, Trojan, time-bombs, keystroke loggers, spyware, adware of any other kind of malware or contamination of computing equipment.

you should carry out your own evaluation/verification exercise before choosing to rely upon any of the content in any way. This does not affect the [weather forecasting agency]’s liability for death or personal injury arising from the [weather forecasting agency]’s negligence, nor the [weather forecasting agency]’s liability for fraud or fraudulent misrepresentation, nor any other liability which cannot be excluded or limited applicable law.

In respect of its conduct with private contracted customers, agencies will also tend to limit liability through clauses stipulating that it is only the minimum service standards specified which need to be met, reliance on the information thereafter is entirely at the customer’s own risk.

Based on the research we conducted, there is yet to be a case in Europe challenging such contractual limitation of liability in this context.

Liability caps:

Were liability ever imposed on the industry in the case of a disastrous occurrence, there is no legal tool or mechanism specifically limiting the extent of the industry’s exposure, beyond best practice, liability-limitation clauses in contracts, and the prevalence of insurance among operators. It is noted also that classic causation requirements are likely to prove difficult from a plaintiff’s perspective in terms of demonstrating causality and so may be limiting to that extent.

Exclusions (force majeure ,etc.):

There is a major issue with this particular industry regarding the extent to which ‘Act of God’ style defenses are likely to hold sway, considering their prediction is the ‘name of the game’, as it were, and that extreme weather events, traditionally considered the definition of ‘acts of god’, are conceivably the very thing which weather forecasting agencies are hired to protect weather-vulnerable enterprises against. It is likely not the case, however, that the ‘Acts of God’ defense to any action would be permissible in all but the most unpredictable circumstances.628

Indemnification:

In terms of general indemnification against reliance upon information by the general public, general disclaimers, as featured above, will also attempt to indemnify the forecasting agency irrespective of the manner in which the information is published or reported. Although any negligence in the manner in which otherwise accurate information is relayed would intuitively rest with the broadcaster, there may be certain issues depending on the extent to which weather forecasting agencies’ staff are called upon to be involved in broadcasting or are called upon as experts, since the conclusion of the controversial L’Aquila Case in Italy of October 2012629, presented in the following paragraphs.

---

628 Millington 1987, p. 238.
629 Procura Della Repubblica Presso il Tribunale di L’AQUILA Proc. Pen. 253/10 R.
In early April 2009, an earthquake of 6.3 magnitude hit L’Aquila in Italy, killing over 300 people.\(^{630}\) In 2012 there followed a case against six scientists specializing in seismology, and one government official, who were charged with ‘providing incomplete, imprecise and contradictory information’ on the risks posed, to the public.\(^{631}\) The technical charge was that of ‘carrying out a superficial analysis of seismic risk, and providing false reassurances to the public’.\(^{632}\) Although no abrogation of duty was found it was alleged that the manner in which the defendants relayed the information about the risk, although they never completely discounted an earthquake, was contradictory and misleading, and responsible for the decisions made by some residents not to evacuate where they otherwise would have done so.\(^{633}\)

The seven defendants, all belonging to the Italian National Commission for the Forecast and Prevention of Major Risks, were sentenced to six years imprisonment each for giving such false assurances, barred for life from holding public office, and ordered to pay compensation of €7.8 million.\(^{634}\) The case is currently under appeal.

The case deals with seismology rather than meteorology but it may signal that liability may be expanded beyond performance of due diligence in the scientific aspect of carrying out meteorological prediction and on to the manner in which that information is relayed. However, in the meteorological contest it is noted that it is often other actors, in the form of television and radio channels or websites which relay the information.

There is a remaining question, however, as to the extent of liability exposure in cases where a catastrophic event follows which goes unpredicted or predicted in a significantly erroneous manner following a failure by a meteorological forecasting agency to perform its contractual duties. For example, agencies often undertake to provide weather updates at regular intervals of a specified dispersion (every hour, two hours, day etc.) If a significant event occurred after the failure of an agency to perform its contractual duties which led to significant third party liability exposure by the meteorological forecasting agency’s customer, related to the lack of information that was available about a weather event, it is at least foreseeable that the meteorological forecasting agency in such a position could be potentially be faced with significant liability exposure.

Insurance:

Insurance is both available and prevalent, with most major weather forecasting agencies carrying public liability and professional indemnity insurance, at the very least.\(^{635}\)

### 6.2.4. Relevance to the Security industry

The actual liability exposure of companies in different sectors of industry varies due to factors such as the nature of their activities, the physical risk associated with such activities, and the law and regulations applying to their activities, including the liability rules. Another factor,
which has been considered in this section of the report, is industry practices with respect to risk management. Three sectors of industry have been reviewed: the software industry, the pharmaceutical industry, and the meteorological industry.

Below, we consider the relevance of these practices to the security industry. One of the primary considerations in attempting to draw useful parallels is the extent to which the mechanisms employed by the sectors of industry surveyed can be said to effectively limit liability within the software, pharmaceutical, and meteorological industries.

6.2.4.1. Software industry

In respect of liability exonerating and liability limiting contracts deployed by the software industry, their EULA’s do, at a basic level, have the power of limiting exposure and minimizing claims. However, they are not enforceable in the European Union to the extent that they seek to limit consumers’ choice of forum or court,\(^636\) nor to the extent to which they seek to impose a limitation on liability for personal injury or death and any incidental or consequential damages arising therefrom under the Unfair Contract Terms Directive. The Unfair Contract Terms Directive provides that: “A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties rights and obligations arising under the contract, to the detriment of the consumer.”\(^637\)

Clickwrap agreements fit nicely within the ambits of ‘not individually negotiated’ agreements, further defined by the Directive under Article 3(2). “A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of pre-formulated standard contracts”.

The Directive requires that such contracts do not contain terms which are ‘unfair’ to the consumer. An illustrative list of those terms which would be considered unfair is also provided.\(^638\) Among them are those terms which have the object or effect of: “excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;… excluding or hindering the consumer’s right to take legal action or exercise any other legal remedy”.\(^639\)

Many EULA’s will acknowledge within their terms that such limitations will not apply in the EU. Others are more general in their acknowledgment of the non-universality of such limitations. See, for example, one cyber security firm’s End User License Agreement, whose limited liability clause attempts to debar access ‘to all damages whatsoever’, is followed with the following acknowledgement:

“BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.”

\(^636\) Article 6, Council Directive 93/12/EEC on unfair terms in consumer contracts (‘the Unfair Contract Terms Directive’): “Member States shall take the necessary measures to ensure that the consumer does not lose protection granted by this Directive by virtue of the choice of the law of a non-Member country as the law applicable to the contract if the latter has a close connection with the territory of a Member State.”

\(^637\) Article 3(1)

\(^638\) Annex 1.

\(^639\) Annex 1, para 1(a) and (q).
Where jurisdictions restrict the ability of EULAs to specify a go-to court for claims, or to limit liability for personal injury and incidental or consequential damages, software companies seem to have no choice but to absorb this liability exposure. However, to the extent that the industry’s current practices manage to comprehensively limit or reduce exposure the evolving nature of the industry, and relatively new circumstances both of its operating procedures and the liability-restricting methods it seeks to employ, remain untested by a major claim, such that relative successes or not can only be speculated upon.

Moreover, although insurance does not in any way limit liability exposure, it does at least provide companies with some assurance when it comes to being able to meet potential future claims and software companies have ready access to such policies.

The software industry has been able to tailor and develop its own liability-limiting practices because as an industry it is in a unique position for a number of reasons:

(i) The nature of the product that is delivered is one which cannot be held to any objective ‘safety’ standards beyond the norm of manufactures and product integrity of the corporeal article. Beyond such it is very difficult to specify what is/is not due diligence when it comes to technologies and threats which are constantly evolving.

Outside of strict design defect it is likely the dynamic and evolving nature of the industry would make causation and due diligence, and duty of care incredibly difficult to specify with certainty. Whilst probably not applicable the Product Liability Directive, for example, provides that a producer cannot be held liable where he can demonstrate that “...the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be detected”.640

(ii) The method of delivery also allows for the utilization of shrink/click wrap agreements due to the often online, as-is nature of the vending process. Linked to this is the respective bargaining power of both parties: software companies cannot profitably sell single use programs without indemnifying themselves against implied statutory warranties (like functionality and security) and limiting the scope of their prospective liability. Because no firm is in a position to do this all providers must offer terms to this effect in their EULAs, thereby normalizing their use and precluding consumers from the opportunity to access such products at all without acquiescing to them.

(iii) The position of contract service providers: when it comes to the provision of bespoke security services for critical infrastructure, certainly the use of such agreements is not to be conceived. Nevertheless, although due to the discreet and sensitive nature of the service involved when it comes to cyber-security for critical infrastructure, for example, information is hard to garner, we can conclude fairly reliably that contractors for these positions, as with other analogous ones in the state-service sector, will have cyber liability insurance policies. Moreover, when it comes to the most vulnerable industries, the likelihood that they are jointly operated with state agents increases, potentially shielding such contractors from sole liability, or bringing them within the frame of sovereign immunity from actions.

640 Article 7(e).
6.2.4.2. Pharmaceutical industry

The pharmaceutical industry remains largely exposed to third-party liability claims in Europe, however, strict regulation and pharmacovigilance procedures, together with an absence of the kinds of class actions suits possible in other jurisdictions, allow it to operate well despite this exposure.

The limited mechanisms which the pharmaceutical industry does employ in Europe are certainly dictated by the size and profitability of the industry when it comes to demonstrating that risks can be absorbed for schemes such as that in Sweden and thus would only be readily redeployable in the context of similar company size, capitalization, and market structures. Moreover, the strict regulation at all stages of production help to limit the likelihood of claims, coupled with the industry’s long experience and history of facing claims, two particular experiences which are not shared by the security industry.

Most particular to the pharmaceutical industry, however, is the nature of the product in question. Pharmaceutical products are sold as ‘inherently’ risky. i.e. it is acknowledged that there are practically no drugs which do not pose some inherent risk to the user. The extent to which the industry is exposed when it comes to such risks will depend on the Member State involved, however, with some, such as Germany, imposing strict liability for any risks not pre-identified which cause personal injury to the plaintiff, whereas others, such as the Swedish model, ask whether in all likelihood the plaintiff would have absorbed the unforeseen risks had they been privy to them. The security industry’s products, by contrast, do not enjoy such a characterization. Although it may be the case that certain products or services may not be, or cannot feasibly be, expected to be effective 100 per cent of the time, it is the case that they are expected to carry out their main function in preventing attacks 100 per cent of the time. To the extent that they are inhibited from doing due to the inherent nature of the product or time and space constraints their inability to perform their function is not likely to fall into the same category of ‘unfortunate side effects’ which the pharmaceutical products may be allowed to.

6.2.4.3. Meteorological industry

In terms of the general user who uses publically available weather information free of charge, the liability limiting clauses and disclaimers employed by the industry are quite effective in limiting liability exposure. However, in situations where such devices were not deployed by the industry, standard tortious defenses relating to the foreseeability of harm and the obligation on plaintiffs to establish causation would likely also insulate the industry to an extent, considering it is almost impossible to predict how such a variety of users are likely to use the information in question.

The liability exposure of the metrological industry is mostly protected by the requirements of tort law. Although the same standards and principles of tort law will likely apply to the security industry in the event of an incident, the burdens placed on plaintiffs in terms of, for examples, foreseeability of harm in a negligence case would likely be far less onerous and comparatively of far less trouble to prospective plaintiffs. In terms of the liability limiting clauses which the meteorological industry uses in contracted work and with the general public, these also play a role in minimizing the industry’s exposure which is again centred on the nature of the prediction service it provides and is thus unlikely to transplant well.

641 Note Finland has legislated specifically to include damages for pain and suffering to be retrieved, although this is not the norm in Europe.
Moreover, it is noted that there remain areas and circumstances in which the meteorological industry remains vulnerable to liability exposure.

The nature of the service by the meteorological industry is that of best prediction rather than best information. Thus the industry will always be insulated to an extent by the uncertainty of scientific processes. However, this is tempered to the extent that ever-evolving meteorological forecasting equipment and processes make prediction more and more certain, coupled with increasing guarantees of accuracy by advertised services in the context of contractual relationships with particular customers. In this sense an analogy can perhaps be drawn with the cyber security industry which has to evolve and work on prediction to an extent in eliminating or prioritizing threats with imperfect information, but otherwise the security industry service cannot be said to enjoy this position, which is central to the meteorological industry’s approach to limiting its liability exposure.

6.2.5. Conclusions Industry Practices in other sectors

Each of the sectors of industry surveyed shows certain specific characteristics that have influenced the nature and extent of the instruments deployed to limit liability and spread the consequences thereof. It is therefore difficult to generalize or extrapolate to the security industry, which operates in different markets, is subject to different laws, regulations, economic forces, etc.

In theory, the contractual mechanisms deployed in the sectors of industry surveyed could be relevant to the security industry or parts thereof. Whether, in practice, contractual liability limitations can play a significant role is a function of whether such limitations will be accepted by the security industry’s business partners, and to what extent such limitations will have effect vis-à-vis third parties that have not agreed to them. This, in turn, is a function of market structure, relative bargaining power, specific laws and regulations, etc. A similar reasoning applies also to the possible deployment of mutual risk pools; in theory, such arrangements could help, but whether, in fact, they could be established by and for the security industry given the industry’s particular idiosyncrasies would require further analysis, not least into whether the industry would support such action, whether there is sufficient standardization across the industry to enable a general standard of risk to be determined, whether the political context in which the security industry operates would support such action, which structures would be most fitting to the industry and, of course, whether other means, or a combination of them, could achieve the same effect in a more comprehensive, cost-efficient or desirable manner.

In short, the analysis of industry practices in other industry sectors provides useful insights into how liability risks can be managed. It demonstrates the respective strengths and weaknesses of each approach for the relevant industry but also highlights the extent to which particular industry practices in this regard are a product of the particular needs and experiences of the industry in question. We understand that contractual mechanisms may be difficult for the security industry to secure because contracts are largely awarded by public procurement based on contracts that are not negotiable. Sector-wide mechanisms are an option, but we have not been informed of any such attempt in the security industry. In this analysis, we are unable to determine whether and, if so, how, specific tools could be relevant and workable in the security industry without delving much further into the industry’s structure, attitudes, experiences, needs, and working context.

642 Millington 1987, p. 238.
6.3. Insurance of man-made disasters and terrorism

6.3.1. Man-made disasters: liability insurance

When referring to man-made, also known as technological, disasters an important feature is that (precisely because they are man-made) in principle there is a tortfeasor who can be identified and be held liable. Hence, the principle instrument to control man-made risk, also when they are catastrophic, is tort law. We are referring here, for example, to the operation of a nuclear plant, but also to risks emerging from petrochemical companies or offshore installations like the Deepwater Horizon.

The insurance scheme that one would primarily look at in this particular situation is then obviously liability insurance. Liability insurance has two main functions. One function is that it protects risk averse injurers from an exposure to liability. Insurance allows the shifting of the risk to the insurance company, thus increasing the expected utility of the insured injurer. In that sense insurance contributes to increasing social welfare. However, since (liability) insurance may create a moral hazard risk the insurer will employ techniques to remedy the moral hazard problem. The first solution is to perfectly monitor the behaviour of the insured injurer and adapt premium and other policy conditions to his behaviour. This will in practice be done via classification and differentiation of risks ex ante and ex post via experience rating systems like the well-known bonus-malus system. In the ideal case the insurer will perfectly control the moral hazard risk as a result of which the insured injurer still has perfect incentives to take optimal care. However, under full insurance coverage his incentives for care no longer come from liability rules directly but from the control of moral hazard by the insurer.

Generally one would assume potential injurers to have a demand for disaster insurance coverage since even relatively large corporations may be averse against the risk of being exposed to catastrophic liability exposure. For smaller liability risks there may not necessarily emerge a willingness to pay the insurance premium especially when the injurer would have alternatives available like creating reserves or captives which may provide protection against liability exposure in a cheaper way than insurance. However, for catastrophic risks even larger enterprises may have a demand for insurance.

Liability insurance may not only be beneficial from the perspective of the potential injurer. A serious problem that victims may face is insolvency of the liable injurer in case of damage of a catastrophic nature. In that case the damage could easily outweigh the personal wealth of the injurer, as a result of which the victims may not receive compensation.

In sum, both potential injurers as well as potential victims may have an interest in having liability insurance for man-made disasters. Insurance can protect risk averse injurers against catastrophic liability risks; insurance can protect the victim against the potential insolventy of

---

643 This corresponds to Task 4.3 of Work Package 4.
644 The liability risks involved in that were already discussed above in 5.2.
645 See for the general features of liability insurance supra section 6.1.3.
646 This is the risk that the insured will behave differently because of the existence of insurance, thereby increasing the liability risk.
647 Experience rating refers to adapting the premium to the behaviour of the insured.
648 This is a system whereby an insured receives a reduction of premium (bonus) when during a particular period no accident was reported or a premium increase (malus) if the insured called on the insurance policy.
649 These methods are in some case referred to as “self insurance”.

209
the injurer and thus guarantee compensation. However, there may be many reasons, as practice shows, why liability insurance for man-made disasters is not always available or not always used.

6.3.2. Demand side problems: the case for compulsory liability insurance

The fact that injurers may not take insurance coverage and thus remain insolvent is in the economic literature referred to as the so-called judgment proof problem. If the injurer would be exposed to liability risks whereby the damage (as a result of the catastrophic nature of the incident) would be a lot higher than his personal wealth an underdeterrence problem emerges. Especially under strict liability (which will often be introduced for these high risk activities) injurers will consider the accident as one with a maximum damage equal to their personal wealth. As a result they will only take care to avoid accidents with a magnitude equal to their own wealth and not necessarily optimal care. Injurers would, from society’s perspective, then be able to externalize harm, i.e. throw the harm on the shoulders of the victims or (if society compensates the victims instead of the injurer) of society at large. Economists have therefore argued that compulsory liability insurance should be introduced in cases where the potential loss caused by the disaster may exceed the injurer’s assets. In cases where the damage caused as a result of a disaster would outweigh the assets of an individual tortfeasor (which may often be the case) there is hence a strong economic argument to impose a duty on potential injurers to provide solvency guarantees (such as insurance) since otherwise they would be able to externalise risk. This potential of externalising harm to society may precisely be one of the reasons why liability insurance for disasters is not purchased as often as it should. Liability insurance after all creates costs for industry (paying the insurance premium) whereas injurers that can externalize harm to society can avoid those costs.

There are quite a few examples showing that in the absence of compulsory liability insurance injurers will often engage in externalisation of harm. For example in some countries in the sector or marine oil pollution it is common practice of a particular fleet of e.g. tankers to create a separate legal entity for each tanker. These are then constructed as so-called “single ship companies”. As a result of the limited liability of corporations in case something goes wrong (like an oil pollution incident) the company has limited its risk to the assets within that particular company which is basically only the ship that caused the marine pollution and will in practice often be worthless or even have a negative value.

Also in other cases there are examples of systematic underinsurance by industrial operators. For example in the Netherlands, following the explosion of a fireworks factory in Enschede on 13 May 2000 that caused 19 deaths and 150 injuries, it appeared that the operator of the factory only had purchased very limited insurance coverage. A few months later on New Year’s Eve in 2000 yet another tragic accident took place in the Netherlands in a bar in Volendam where as a result of a large fire many youngsters died and many were injured for life as a result of burning wounds. Again, the owner of the facility had only very limited insurance coverage.

---

650 Of course other legal issues would still have to be regulated, such as inter alia a direct right of action of the victim on the insurer and a guarantee that the insurance monies can actually be spent for victim compensation for example in case of bankruptcy of the injurer after a disaster.
651 See Shavell 1986.
653 Discussed in more detail above in section 5.3.
This risk of externalisation of harm may hence explain to some extent underinsurance of catastrophic risks. Operators may prefer not to take insurance coverage for high amounts above their own assets for which they could anyway never be held liable in case of an accident because they would be insolvent. Some legal systems do have compulsory liability insurance for particular activities, but it is rather limited. For example compulsory environmental liability insurance existed in Europe (before the implementation of the ELD) effectively only in Germany, Sweden and Spain. Compulsory liability insurance for the risk of fire in public places such as nightclubs and restaurants exists in Belgium, but not in the Netherlands. This led a Belgian commentator to the conclusion that were the tragic fire to have taken place in a bar in Volendam (the Netherlands) on New Years’ Eve in 2000 in Belgium, victims would have been compensated largely through the compulsory liability regime.

6.3.3. Supply side problems

That there is little liability insurance for man-made disasters is not only related to problems on the demand side, but also on the supply side. As will be explained in further detail below, insurers consider catastrophic risks understandably as “difficult to predict”. Insurers may thus have what is referred to as insurer ambiguity which may limit insurability. As a result of insurer ambiguity insurers will add a risk premium and hence ask higher total premiums for catastrophic risks which may not lead to a willingness to pay on the side of industry as a result of which a market may not emerge. In other cases insurers may impose very strict conditions or exclusions which may reduce the availability of catastrophe liability insurance. Finally, the magnitude of the damage of a particular catastrophe may also outweigh the capacity of the private insurance market, even if the possibilities of co- and reinsurance are taken into account.

In sum: insurers may (understandably), given the hard to predict nature of catastrophes, lacking statistics and the potentially high magnitude of the damage be reluctant to provide large coverage for liability insurance for man-made disaster or may only do so at high premiums or with particular exclusions which may make the insurance unattractive.

6.3.4. Government support needed?

One of the reasons for a relatively limited market for liability insurance of man-made disasters may be related, as we just argued to problems on the supply side. If it is more particularly the catastrophic nature of the damage which may restrict the possibilities of (re)insurance and financial markets to cover catastrophic risks, the government may intervene actively with a facilitative strategy to support the functioning of the private insurance market. This could take various forms. In some cases the government may act as insurer of last resort; in other cases the government could provide reinsurance in cases where capacity on the traditional reinsurance market is lacking.

---

655 Recall that also in Chapters 3 and 4 we examined to what extent compulsory liability insurance exists and found out that this is only to a limited extent the case.
656 For an overview of the German system see inter alia Richardson 2000 and for a description of the Swedish system see Faure and Grimeaud 2003, p. 189-192.
658 When discussing supply side problems in case of natural disasters in 6.4.4.
659 See Gollier 2005.
660 See Kunreuther, Hogarth and Meszaros 1993.
6.3.4.1. The case for public-private partnerships

Both in law and economics and in legal scholarship criticisms have been formulated on the facilitative role of a government stimulating insurance markets.\(^{662}\) Gron and Sykes argue that it would be unjust for the government to provide (re)insurance at a lower price than the market price.\(^{663}\) This would give a wrong signal to the market as far as stimulating insurability is concerned. The authors would prefer ad hoc solutions whereby compensation is provided to accident victims on an ex post basis. This would avoid the situation that market participants are aware that the government will anyway guarantee compensation.

Also Dutch lawyers, Ammerlaan and van Boom, have been critical of an intervention by the (Dutch) government to participate in reinsurance against terrorism. They argue that the premium that will be demanded is not a correct premium. Moreover, they argue that it should not be the task of the State to provide private insurance. Damage caused as a result of terrorism, so they hold, should be financed through the public purse.\(^{664}\)

It is striking that most of this criticism is not addressed against the intervention of the government as such, but is based on the assumption that the government will not ask premiums that reflect market prices. It is a criticism shared by Levmore and Logue, who argue that such a regime (of acting as reinsurer of last resort) only has its desired effect of encouraging the purchase of commercially provided terrorism coverage when it involves a substantial subsidy.\(^{665}\) They are skeptical of these types of interventions in the market (for terrorism insurance) arguing that, also without government intervention, “the market would likely have been able to provide the necessary coverage”.\(^{666}\)

Apparently, the arguments against government intervention are based on the assumption that the government will not ask competitive reinsurance premiums, hereby subsidizing catastrophe insurance. Moreover, without this government support, insurance coverage could have probably developed anyway (at least for terrorism events). Those points can of course only be validated on the basis of empirical research.

The arguments in favour are hence not surprisingly the mirror image of the arguments against: assuming that capacity on the private insurance market is indeed severely falling behind, it can be assumed that without State intervention, insurance coverage for disasters would simply not have developed.\(^{667}\) Reinsurance by the State can then be considered as an adequate method to resolve the uninsurability problem. A condition is of course that the government charges an actuarially fair premium for its intervention.\(^{668}\) This type of government intervention has, moreover, the advantage that ex post relief sponsored through the public purse can be avoided. Where the government acts as reinsurer, this at least has the advantage that a premium can be paid by those who actually cause or run the risk. It can thus facilitate market solutions, still provide incentives for prevention to potential victims and avoid negative redistribution. Thus a State intervention as reinsurer may avoid the “catastrophic responses to catastrophic risks.”\(^{669}\) This is further supported by the fact that in case of this type of government provided reinsurance the government has the capacity to

\(^{662}\) See Trebilcock and Daniels 2006.
\(^{663}\) See Gron and Sykes 2002 and Gron and Sykes 2003.
\(^{664}\) Ammerlaan and Van Boom 2003.
\(^{665}\) Levmore and Logue 2003, p. 304 (arguing that otherwise disaster insurance would still not be “available”).
\(^{666}\) Levmore and Logue 2003, p. 311.
\(^{667}\) This is a point strongly made by Kunreuther 1996, p. 180-183; Harrington 2000; as well as by Schwarze and Wagner 2004.
\(^{668}\) Faure 2007, p. 358.
\(^{669}\) Epstein 1996. See in this respect also Kunreuther and Pauly 2006, p. 113 (arguing that this government’s role in assisting the supply side allows avoiding the inefficiencies and inequities associated with disaster assistance).
diversify the risks over the entire population and to spread past losses to future generations, thus creating a form of cross-time diversification which the private market could not achieve. On the other hand, they argue that, especially as far as terrorism is concerned, government participation in insurance programs is crucial since the risk of terrorist attacks is partly in the government’s control and the government can have more information on ongoing terrorist groups’ activities through intelligence services.

Although there is still some criticism on this intervention of government in providing reinsurance coverage one can notice this type of government intervention in an increasing way, not only in the case of man-made disasters and terrorism but also in the case of natural disasters. However, the literature has indicated that this type of role of government as (re)insurer of catastrophic risks can only be considered efficient when particular conditions are met. These conditions are inter alia the following:

- the intervention by government should not distort the normal functioning of the market;
  when government provides reinsurance risk-based premiums should be charged;
- the government intervention should be such that it stimulates the development of market solutions;
- freedom should be left with insurers to choose the statutory insurance and
- the government intervention should in principle have a temporary character.

If these conditions are met it would be possible that government provides efficient reinsurance stimulating the supply of catastrophe insurance. However, as some of the actual cases of government intervention show government intervention rarely fully complies completely with those conditions.

6.3.4.2. Government providing an additional risk layer: nuclear and oil

One example of government support foresees a role of the government to finance catastrophic damages through an additional risk layer, outside of the insurance market and on an ex post level, above the injurers’ own financing. Such a scheme aims at supplementing compensation from injurers (if needed) and thus at maximising the protection of victims in case the damage exceeds certain limits. In this case the role of the state is merely to guarantee an additional layer of compensation and it adds little as far as facilitating insurability is concerned.

Examples are of course the cases of nuclear liability and marine pollution liability discussed above.

As we already made clear, when discussing those international conventions that these models do not at all comply with an efficient government support to stimulate insurability. The goal of providing an additional risk layer is also not to stimulate insurability. The main problem is that the government does not charge any price for providing the additional funding; the intervention does not have a temporary character, market solutions are not stimulated by

---

672 To be discussed below in section 6.3.5.
673 See below in section 6.4.
674 For a summary of those conditions see Bruggeman, Faure and Fiore 2010.
675 See in this respect also the cases discussed in 6.4.5. concerning insurance of natural disasters.
676 In section 5.2 (nuclear liability) and section 5.3 (marine oil pollution).
providing government intervention and the government intervention can in that sense largely
be considered as distortive.\textsuperscript{677}

In fact the domains of nuclear power and marine oil pollution are the rare ones where specific
statutory measures have been taken to deal with the insurability of liability for damage caused
by man-made disasters that is to say that government intervenes where insurability is limited.
Some of the other cases also relate to civil aviation.\textsuperscript{678} Before turning to the specific case of
terrorism we will present two examples of how industry (supported by government) has dealt
with particular catastrophic losses following from man-made disasters. We discuss a
reinsurance arrangement with state intervention that has been created in Spain and we briefly
discuss the Fukushima case.

6.3.4.3. \textit{The Consorcio de Compensación de Seguros}

The Spanish program offers a good example of a government collecting a fee or premium in
exchange of the provision of insurance coverage. The publicly administered disaster financing
program “Consorcio de Compensación de Seguros” (CCS) was founded in 1954 as a
corporation providing ‘extraordinary risks’ insurance, namely coverage against natural
disasters and risks with “social repercussions” (terrorism, riots, etc.).\textsuperscript{679} The Consorcio in fact
acts as a catastrophe insurer for certain types of insurance and perils in respect of Spanish
risks, compensating losses and injuries arising from extraordinary events taking place in
Spain and affecting risks located in Spain. It also covers personal damage for extraordinary
events taking place abroad if the insured resides habitually in Spain.\textsuperscript{680} This extraordinary risk
coverage is a mandatory additional coverage added to fire and natural perils, motor and
railway vehicles and other property damage policies. The extra CCS premium is
automatically included in the base policy’s premium and varies according to the type of
policy offered, although it reflects the base rate charged on the primary policy. Until 1987,
disaster insurance premiums were calculated as a percentage of property damage insurance
premiums. However, since this meant that the premium income was influenced by events
unrelated to disaster insurance, the CCS has set its own, not risk-related and equal for the
entire country, premium since 1987. The extra premium to a personal insurance policy
amounts to 0.005 per mille, while that to a property insurance policy differs: 0.08 and 0.12
per mille of the total sum insured for houses and office buildings respectively; 0.18 per mille
for businesses; 0.21 per mille for industrial risks; € 3.5 for vehicle insurance; and between
0.28 and 1.63 per mille for infrastructure.\textsuperscript{681}

CCS payments are subsidiary to payments made by the private insurance industry and the
Consorcio only pays if the risk was not covered by private insurance (e.g. for the poor who
didn’t buy insurance) or if the private insurance company fails to pay due to insolvency.
Typically, domestic insurers in Spain do not cover extraordinary risks but issue policy
documentation clearly stating that such losses are not their responsibility, but that of the
Consorcio, to whom relevant claims should be addressed. Deductibles for property loss
amount to 7\% of the amount of the indemnifiable damage.

\textsuperscript{677} As we discussed in Chapter 5 this criticism mainly applies to the nuclear liability conventions since the
additional funding is there provided as a state subsidy. See 5.2.8.2; however, in the case of marine oil pollution the
additional funding is not paid by the liable ship owner, but by the oil industry, hence still by a market participant
(see 5.3.8.2.). In fact in the marine oil pollution case there is in principle no government financing.
\textsuperscript{678} Equally already discussed in Chapter 5, in 5.1.
\textsuperscript{679} Over time, the activities of the CCS were extended beyond this core function.
\textsuperscript{680} Estatuto Legal del Consorcio (Legal Statutes of the Consorcio), approved by Law 21/1990 dated 19th
December.
\textsuperscript{681} See: \texttt{<http://www.consorseguros.es/web/guest/ad_re_er>}. 

214
The legal nature of the CCS changed in December 1991, following Spain’s accession to the European Community, from being a State monopoly institution to a public business institution, attached to the Ministry of Economy and Finance. The CCS now has its own legal personality, full capacity to act, and its own assets independent from the State’s. In addition, given the peculiar characteristics of the Consorcio’s activity, and especially given the high loss potential and the very nature of the Consorcio as a public organism, it is absolutely necessary for the Consorcio to count on an unlimited State guarantee. However, the setting up and appropriate financial management of its resources has always enabled it to face up to its claims obligations without having had to make use of said guarantee in the more than half-century that it has been in existence.

6.3.4.4. The Fukushima case

We will briefly discuss the Fukushima case, not only because it is a large scale and very recent (March 2011) man-made disaster, but also because it follows a different structure than the compensation under the nuclear liability conventions discussed in Chapter 5. There are a few features of the insurance and reinsurance structure as well as the state intervention that make the Fukushima case interesting. A detailed discussion of this case would obviously be beyond the scope of this study. We focus on the main features and refer to the literature for further details.

Japan is not member of the international nuclear liability conventions but has an Act on compensation for nuclear damage of 1961. Nuclear operators can still be held liable for the nuclear damage caused by a natural disaster such as an earthquake or volcanic eruption, but they can cover such losses through an indemnity agreement with the government. Since insurers usually exclude the damage caused by natural disasters from liability insurance policies, this kind of risk is covered by an indemnity agreement concluded with the government. A major difference between the Japanese regime and the international regime is that in Japan the liability of the nuclear operator is unlimited. Although there is a minimum for the requirement of financial that has to be provided by the operator, he is still liable for damage in access of that amount. This indemnity agreement is hence a contract that the nuclear operator makes with the government with the view to cover damage which is not covered by liability insurance or other means of financial security. This is mostly for damage caused by natural disasters. It is important that the operator has to pay the government an indemnity fee. The Japanese state hence intervenes in the compensation for the victims of a nuclear accident on the basis of an indemnity agreement for which the operator pays a fee to the state. However, if the damage is still higher than the amount of the indemnity agreement, the state could intervene under section 16 of the Act on Compensation. This state intervention then still takes place on the basis of a political decision.

Looking now at how compensation will take place in the Fukushima case the picture is slightly more complicated. According to the Act on Compensation, the nuclear operator faces

---

682 A full discussion of the Fukushima case can inter alia be found in Weitzdörfer 2011; Faure and Liu 2012a and Faure and Liu 2012b.
683 See Act on Indemnity Agreements for Compensation of Nuclear Damage, Act No. 148 of 1961, para. 3.
684 The Act on Compensation for Nuclear Damage, paras. 6-7.
685 Section 16 states:
[w]here nuclear damage occurs, the Government shall give a nuclear operator (except the nuclear operator of a foreign nuclear ship) such aid as is required for him to compensate the damage, when the actual amount which he should pay for the nuclear damage pursuant to Section 3 exceeds the financial security amount and when the government deems it necessary in order to attain the objectives of this act. Act on Compensation for Nuclear Damage § 16(1).
unlimited strict liability and has the obligation to seek financial security up to 120 billion yen. If the damage is caused by an earthquake or volcanic eruption, the government should indemnify losses up to the 120 billion yen minimum financial security requirement. For damages exceeding this amount, the operator is still liable.

Beyond simply defining the scope of compensable damage, the question exists how this compensation can be financed. Nuclear damage caused by a natural disaster is excluded from the insurance policy provided by JAEIP. Thus, the insurance industry does not seem to be seriously impacted by this accident. The government may have to indemnify the losses up to 120 billion yen. The remainder of the damage may still create a challenge to the financial capacity of TEPCO. According to the Act on Compensation, if the operator’s liability exceeds the amount of financial security and the government deems it necessary in order to attain the objectives of the Act, the government shall give aid to the operator. However, whether and to what extent aid will be given depends on the government’s decision. Because of the significant impact of the Fukushima accident and the catastrophic nature of the damage, it will be difficult for TEPCO alone to provide full compensation.

To ensure a prompt compensation of the damage caused by the Fukushima accident, the government prepared a law to address compensation through the creation of a corporation in June 2011. The Act to Establish the Nuclear Damage Compensation Facilitation Corporation was passed on August 3, 2011. The Act has three aims: ensuring the prompt and proper nuclear damage compensation for affected people, stabilizing the nuclear power station to prevent adverse effects on life and commerce in the surrounding area, and maintaining a stable supply of electricity. To realize those aims, the Act establishes a Nuclear Damage Compensation Facilitation Corporation (“the Corporation”) and a system of financing the compensation for damage. The Corporation will receive contributions from nuclear operators to cover the costs of operation, and reserve funds to prepare for compensation. The victims still need to make a claim against the liable operator, and the liable operator needs to make the payment to the victims. However, the Corporation can facilitate the compensation and “provide . . . necessary information and advice” to the affected people. If the liable operator needs assistance, the Corporation can provide two forms: ordinary financial assistance, which can be given after a resolution of the management committee of the Corporation; and special financial assistance, which needs to be approved by the competent minister. To obtain the special financial assistance, the Corporation and

---

688 This is the insurer of the nuclear risk in Japan.
689 Act on Compensation for Nuclear Damage § 3.
690 Act on Compensation for Nuclear Damage § 16.
693 Id.
694 Id.
695 Id.
696 Id., p. 3.
697 See METI Outline, supra note 386, p. 2.
the operator need to formulate a special business plan. Under this plan, the government will issue government bonds to the Corporation and the Corporation will grant the necessary funds to the nuclear operator. The Corporation can also get government backed support from financial institutions. After getting this support, the liable nuclear operator pays special contributions to the Corporation. Other non-affected nuclear operators also need to pay general contributions based on the principle of “mutual support.”

This Act established a mutual support “pooling system” to provide coverage for nuclear liability after the Fukushima accident. Some scholars advocate pooling as a useful instrument to finance the compensation of catastrophic losses while preserving preventive incentives. The mutual support system established in Japan has some characteristics different from the practice in other jurisdictions. In both Germany and the U.S., where resource pooling between nuclear operators has been established, pooling is done before accidents happen. However, the ex post system established in Japan cannot create incentives among operators to monitor each other. Unlike the American and German regimes, under the Japanese system the Corporation is not only financed by nuclear operators, but also by government compensation bonds and government guaranteed bonds. If those funds are financed without a market price, this system will look more like a bailout of TEPCO than a pooling system to prevent and compensate for future damage.

This compensation scheme in Japan hence has a few interesting features. Though the Act on Compensation does not set a cap on the potential liability of nuclear operators, the corporate structure only exposes them to risk up to the value of their assets. In this situation, a financial guarantee is important to ensure efficient deterrence. In Japan, the required financial security is set at 120 billion yen. This amount is provided through a combination of liability insurance, for which the operator will pay a premium, and an indemnity agreement with government, for which a fee will be paid as well.

Compensation under this indemnity agreement is not a mere subsidy. However, the indemnity fee charged for government coverage is certainly not market based. On the contrary, the fee is fixed, and therefore not risk related. Moreover, though the operator remains liable beyond the insured amount of 120 billion yen (except when the incident would be qualified as a natural disaster of an exceptional character) the exposure to liability of the operator is de facto limited to its assets. Beyond that amount, Japanese law provides that government may use its discretionary powers to “take measures,” meaning that it will intervene to compensate victims. In that case a lack of full internalization of the accident costs remains a problem. This still raises the question to what extent a nuclear operator like TEPCO is fully liable for accident costs and to what extent liability rules do provide adequate incentives for taking preventive measures with a view to cost internalization.

---

698 Id.
699 Id., p. 2-3.
700 Id.
701 Id., METI Outline, p. 3.
702 Id., Nuclear Damage Compensation Outline, supra note 385.
704 See Pelzer 2007, p. 49.
706 See Ramseyer 2011, p. 3.
707 Id., p. 8.
708 See Act on Indemnity Agreements for Compensation of Nuclear Damage, §§ 2-4, 6.
709 Id., § 6.
710 See Ramseyer 2011, p. 17-18.
711 Act on Compensation for Nuclear Damage, §§ 16-17.
As far as the financing is concerned, Japan’s program seems to do better than the international regime at compensating victims. As we have indicated above (in section 5.2) currently, of the total amount available under the international regime of € 381 million, only € 91 million consists of operator’s liability, whereas the remaining € 290 million consists of state aid.\footnote{Even after the entry into force of the modification protocol of 2004, only € 700 million of the total amount of € 1.5 billion would be operator’s liability and a remaining € 800 million would still be state aid. Yamori and Okada 2007 and accompanying text. See above 5.2.8.2 for the funding of nuclear liability in the international regime.} In Japan this amount of 120 billion yen is in principle paid by the operator, either (in the general case) via liability insurance or, in case of uninsurable risks (more particularly damage resulting from earthquakes, tsunamis or volcanoes) via an indemnity agreement with government.\footnote{See Ramseyer 2011 and the Act on Indemnity Agreements for Compensation of Nuclear Damage, §§ 2-4, 6 and accompanying text.} But the indemnity agreement is, unlike state aid in the international regime, not a subsidy since the operator has to pay a fee for the coverage provided by government via the indemnity agreement.

Of course one could question whether the fee paid by the operator for the indemnity agreement is comparable to commercially risk dependent premiums that would be charged on a commercial insurance market. One report shows that in 1998, the premium rate was set at an average of 7.9 percent of the total amount of coverage,\footnote{Watabe 2006, p. 222.} which is substantially higher than the rate of indemnity fee (0.03% or 0.015%).\footnote{Order for the Execution of the Act on Indemnity Agreements for Compensation of Nuclear Damage § 3.} However, it should be born in mind that given the lack of actuarial data for nuclear accidents, commercial premiums are usually set higher than the actuarial premium. Thus the difference between the rate of indemnity fee and actuarial premium - a more accurate measure of risk - may not be that large. On the positive side, at least in Japan, some money is asked from the operator for the government indemnity, whereas in the international regime the state aid is provided for free - functionally, a complete subsidy. Therefore less subsidy is given under the Japanese system. Moreover, unlike the international regime there is in Japan in principle unlimited liability of the operator beyond the amount of 120 billion yen,\footnote{Weitzdörfer 2011, p. 70-71.} for which the operator must seek either liability insurance or an indemnity agreement. Hence, the Japanese system has less of a subsidy effect than the international regime, and thus better prospects of cost internalization by the operator.

6.3.5. Terrorism

Finally we will focus on one particular type of technological or man-made disaster, being a risk which plays an important role for the security industry, terrorism. Terrorism has many features that make it look more like a natural disaster (to be discussed in the next section) than like a normal man-made disaster. The simple reason is that in case of terrorism normal liability rules cannot be applied since the terrorist will usually not be identifiable or if he is, he will usually be insolvent. Moreover, remedies we suggested above with respect to liability for man-made disasters, such as compulsory liability insurance, of course do not work in the case of terrorists either.

The reason to look specifically at the case of terrorism is that terrorism insurance has dramatically changed after 9/11. After that date insurance companies began massively cancelling terrorism coverage (usually on first party insurance policies, but also related to airline insurance).\footnote{See Hartwig 2002.} As a result of that cancellation in many countries systems emerged where the state often took the role as reinsurer of last resort. Public-private partnerships were
created whereby terrorism coverage consisted of several layers with an intervention by the insurers, reinsurers and government. However, the way in which terrorism insurance emerged in different countries is quite interesting since it shows again how government can facilitate the functioning of the market mechanism and more particularly insurance. Of course we do not have the possibility to discuss all new terrorism insurance schemes that emerged after 9/11. We already referred to the CCS in Spain where the CCS provided terrorism cover until 31 October 2000 after which the cover became available on the private market. Examples also exist inter alia in the United Kingdom where reinsurance is provided through pool re. We will present the insurance schemes for terrorism in the US, France and the Netherlands.

6.3.5.1. Tria

The American Terrorism Risk Insurance Act of 2002 (“TRIA”) establishes a temporary program of shared public and private compensation for insured losses resulting from foreign acts of terrorism in order to “protect consumers by addressing market disruptions and ensure the continued widespread availability and affordability” of terrorism insurance, and to “allow for a transitional period for the private markets to stabilize, reserve pricing of such insurance, and build capacity to absorb any future losses (...).” TRIA creates a federal backstop for terrorism insurance, meaning that federal financial support is provided for payment of terrorism claims in the event of a fairly large terrorism incident. The program is similar to reinsurance in that it provides reimbursement to insurers after they pay claims to a specified level (the deductible) and in that insurers retain a portion of the risk (a co-pay). However, a difference with reinsurance is that insurers do not pay a premium to be eligible and the government does not establish any reserves. Instead, the costs of the TRIA program are born by the taxpayers with some or all of the costs subject to recoupment. In short, the Terrorism Risk Insurance Act of 2002 offers an illustration of the federal government providing coverage above a baseline risk that remains under the coverage of private insurers. The federal government temporarily assumes the role of excess liability insurer (i.e. reinsurer of last resort), providing a cap on the losses for which the private insurance industry remains responsible in the event of a terrorist attack. The program would initially exist for two years, with the expiration date set at 31 December 2005, but has been systematically extended ever since.

All insurers providing commercial property or casualty insurance are required to participate in the program as elaborated in the Terrorism Risk Insurance Act of 2002. The insurers must make terrorism insurance available to all policyholders, but are free to choose the applicable extra terrorism premium, which should not be excessive, inadequate or fairly discriminatory.

718 See above 6.3.4.3.
719 See Huber and Amodu 2006.
720 The TRIA act does not cover any of the September 11th losses.
722 Rabin and Bratis 2006, p. 325.
723 TRIA only applies to commercial property and casualty insurance, which is defined to specifically include excess insurance, workers’ compensation insurance, and during the first three years of the TRIA Program, surety insurance. (Workers’ compensation insurance mandatorily includes insurance against terrorism, even without TRIA. See Hockman, Lowe, et al. 2004. Workers’ Compensation Terrorism Reinsurance Pool Feasibility Study. Tillinghast and Reinsurance businesses of Towers Perrin, for how workers’ compensation can deal with the problem of terrorism losses). TRIA does not apply to personal insurance, such as homeowners’, automobile or life insurance. Moreover, by law, the TRIA program does not apply to: federal or private crop insurance; private mortgage insurance, or title insurance; financial guaranty insurance offered by a monoline financial guaranty insurance corporation; insurance for medical malpractice; health or life insurance, including group life insurance; federal flood insurance; and reinsurance or retrocessional reinsurance.
If a certified foreign act of terrorism causes losses in excess of $100 million, participating insurers must pay a certain amount in claims – a deductible – before federal governmental assistance can become available. This deductible is now set at twenty percent of the insurer's directly earned premiums during the preceding year. Losses above the deductible will for 85% be covered by the federal government, while the insurance industry contributes 15%. An annual cap of $100 billion to all aggregate insured losses has been installed. In case the cap would be exceeded, Congress has the authority to decide who will pay and in what amounts: the Secretary shall determine the pro rata share of insured losses to be paid by each insurer that incurs insured losses under the program. Insurers that meet the deductible will not be liable for losses in excess of this cap.

6.3.5.2. GAREAT

French primary insurers that offer fire insurance are required by law to also provide terrorism coverage. In practice, coverage against acts of terrorism was generally included in all standard insurance policies, which means that all private and commercial properties were generally covered against terrorism events. However, after the September 11th attacks, reinsurers cancelled their terrorism coverage and many primary insurers that could not obtain reinsurance chose to stop offering (especially commercial) property insurance to avoid the mandatory terrorism coverage. According to French insurance industry officials, the French government responded to this situation by, first, temporarily requiring the extension of all contracts, and, second, beginning negotiations with the insurance industry to develop a more permanent solution. As a result, the ‘GAREAT’ (‘Gestion de l’Assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme’) reinsurance pool was created jointly by insurers, reinsurers and the Caisse Centrale de Réassurance on 1 January 2002. The idea is based on the existing administrative structures of the insurance associations and the natural catastrophe program already in place in France. The goal of GAREAT is to cover acts and attacks of terrorism (including those involving the use of nuclear weapons) which cause damages on French territory (and assimilated territories).

Though GAREAT membership is not mandatory for insurance companies operating in France, insurers affiliated to FFSA (the national association of insurance companies) and GEMA (the main trade body for mutuals) automatically qualify as members of the pool. Upon subscription to GAREAT, each member is liable in proportion to the amount of the premiums ceded to the pool in respect of the subscription year.

The GAREAT program is divided into two sections: the ‘Large Risks’ section and the ‘Small and Medium-Sized Risks’ section. The Large Risks section entails all contracts which fall within the scope of application of the GAREAT pool and whose sums insured for direct property damage, business interruption, and construction, engineering and financial institution lines are in excess of € 20 million. The pool’s Large Risks section is in other words limited to commercial, professional and industrial risks where the sums insured are equal to or greater than € 20 million. The Small and Medium-Sized Risks section, on the other hand, includes

725 For all information on GAREAT, see: <http://www.gareat.com/gareat/rtaccueil.nsf/documentation?Openpage>, which includes the Internal Rules, Co-reinsurance conventions, Statutes, etc. of the pool programme.
726 GAREAT’s scope of application is broader than the obligatory coverage resulting from Article L. 126-2 of the Insurance Code. The following additional contracts are, inter alia, included: contracts reinsuring policies underwritten by captives and falling within the scope of application of Article L. 126-2 of the Insurance Code; contracts which cover solely business interruption arising out of an act of terrorism but which do not fall within the scope of application of Article L. 126-2 of the Insurance Code because they provide no fire coverage; and insurance contracts whose main purpose is specifically to cover risks relating to acts of terrorism.
those contracts which fall within the scope of application of the GAREAT pool and whose total sums insured are less than €20 million. The Small and Medium-Sized Risks section will not be further discussed in the following, since properties less than €20 million may be ceded to the pool on a voluntary basis.

Both sections are the subject of specific provisions and each section is divided into layers. GAREAT’s structure may then briefly be described as follows:

1. the first layer of the program consists of co-reinsurance between the members of the pool. The losses to this layer are split between the members proportionally to their respective shares of the section in question;
2. the next layers consist of reinsurance by professional reinsurers, who provide capacity in the form of Annual Aggregate Excess of Loss treaties. For the Large Risks section, the members of the pool may participate in these reinsurance layers. These layers are the subject of reinsurance treaties;
3. the top layer consists of, for the Large Risks section, unlimited reinsurance granted by the Caisse Centrale de Réassurance with a guarantee from the French state. This layer is the subject of a reinsurance treaty with the CCR. The CCR receives for this purpose a premium from GAREAT.

For the year 2012, the co-reinsurance layer has a limit of €400 million for the entirety of the losses. The second, third, fourth, and fifth layers constitute the Annual Aggregate Excess of Loss reinsurance program taken out by GAREAT on the international reinsurance market. The second to fifth layers are each limited to €400 million. The sixth layer constitutes the top layer where the CCR provides coverage (with an unlimited guarantee from the French State) in excess of a loss threshold of €2 billion.

727 The scope of application of GAREAT is not exactly the same as that one of the top layer which is reinsured by CCR with the French State’s guarantee. The scope of application of the CCR corresponds to that of Article L. 126-2 of the Insurance Code, which does not include (or which excludes) a certain number of risks which are covered by GAREAT. Coverage for railway vehicles and coverage for business interruption following a shortage in supplies, for example, do not enjoy the CCR’s unlimited coverage. The risks which do not fall within the scope of application of the top layer are co-reinsured by the members of the pool in the same conditions as those applicable to the first (co-reinsurance) layer. The functioning of the CCR will be discussed in further detail below in 6.4.5.1.
The premiums paid to GAREAT are intended to cover: 1) the premiums paid to the members and reinsurers participating on the various reinsurance layers; 2) the premiums paid to CCR; and 3) GAREAT’s operating expenses. The GAREAT premiums, paid by its members, are calculated independently of the terrorism insurance premiums these members charge under the contracts issued by them. With regard to the risks ceded to the Large Risks section, the GAREAT premiums are, in principle, calculated by multiplying the GAREAT premium rates, which vary according to the sums insured, by the total amount of the insurance premiums received by GAREAT. The premium to be paid to GAREAT is thus: GAREAT premium rate \times\text{premiums collected}.

The GAREAT premium rates are indeed fixed by reference to the amount of the sums insured:

<table>
<thead>
<tr>
<th>Amount of total sums insured</th>
<th>GAREAT premium rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum insured &lt; € 6 mio (facultative session)</td>
<td>3 %</td>
</tr>
<tr>
<td>€ 6 mio &lt; sum insured &lt; € 20 mio</td>
<td>6 %</td>
</tr>
<tr>
<td>€ 20 mio &lt; sum insured &lt; € 50 mio</td>
<td>12 %</td>
</tr>
<tr>
<td>€ 50 mio &lt; sum insured</td>
<td>18 %</td>
</tr>
<tr>
<td>sum insured &gt; € 750 mio</td>
<td>quoted individually</td>
</tr>
<tr>
<td>nuclear risks</td>
<td>24 %</td>
</tr>
<tr>
<td>exceptional risks (e.g. captives)</td>
<td>special rating</td>
</tr>
</tbody>
</table>

Consequently, GAREAT earned in 2007 252 million EUR in premiums on 105,000 policies.

---

The Dutch government and the Dutch Association of Insurers agreed to set up a dedicated reinsurance company, called the Dutch Terrorism Risk Reinsurance Company or ‘NHT’ (‘Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden’), to cover insurance against terrorist acts in all classes of business.\textsuperscript{729} This step represented an intervention measure to address a market failure following the limited supply of terrorism risk cover.

Since 1 July 2003,\textsuperscript{730} more than 250 insurance companies (i.e. 93\% of all active Dutch insurers), together with the government and some reinsurance companies, participate in NHT. The participating insurance companies are deemed to cede all their terrorism exposure (irrespective of the category of insurance contract) to the NHT pool, which acts as a reinsurance company. The overall capacity of the terrorism risk reinsurance pool is limited to € 1 billion per calendar year. It was foreseen that this threshold of € 1 billion would be gathered in three layers: the first € 400 million will be reinsured by the participating primary insurers (even in case a particular insurer does not need to collect revenues from the NHT), while losses in excess of € 400 million in the annual aggregate will be protected under a reinsurance market excess of loss programme valued at € 300 million, with any shortfall taken up by the Dutch government, acting as a reinsurer of last resort, up to another € 300 million. In the first layer applies, moreover, a so-called threshold deductible, meaning that all terrorism damage under the amount of € 7.5 million belongs to the own risk of the insurers, although this clause has not been laid down in the official regulations. All in all, the solidarity principle among the insurance companies is an important aspect of the NHT – participation in the pooling construction is after all not mandatory, although the non-participants will be followed closely and critically by the supervisor PVK (‘Pensioen- en Verzekeringskamer’).

Further, in order to prevent that a large damage with one insured in one location would monopolize the total capacity of the NHT pool, a premier risk amount of maximum € 75 million will be insured per location and per insured, for all participating insurance companies together, irrespective of the number of insurance contracts issued.

The Dutch government asks a premium for its reinsurance capacity which is chosen in such a way that it will price itself out of the market at the time insurability of the terrorism risk is restored. From the period of 1 July 2003 until 31 December 2003, the government asked a premium of € 10 million (i.e. € 20 million on a yearly basis).\textsuperscript{731} A system of various portions is hereby operated, whereby the first part of coverage is relatively expensive: the first portion of € 100 million demands the same premium as the second portion of € 200 million. After all, an incentive is hereby incorporated in order to stimulate the recovery of commercial insurance: in case individual reinsurers would be capable to cover the risk, expectations are that they would offer this coverage against a lower premium. In case of recovery of the commercial insurability the government would indeed price itself out of the market. This point of departure indeed seemed to have started to pay off since a commercial reinsurer declared itself willing to cover the first € 100 million of governmental coverage (namely between € 700 and 800 million), so that governmental intervention was decreased to € 200 million.\textsuperscript{732} Moreover, since 1 January 2006, the Dutch government only needs to guarantee € 50 million in case the NHT compensates for more than € 950 million.\textsuperscript{733}

\textsuperscript{730} The NHT became operational on 1 July 2003. It has been periodically extended for additional periods, and is expected to be further extended as long as market conditions require.
\textsuperscript{732} Parliamentary Proceedings of the Second Chamber of Representatives 2002-2003, 28 915, No. 5, 12 August 2003, p. 3.
6.3.6. Conclusions Man-Made Disasters and Terrorism

This chapter presented theoretical and empirical insights in the approach insurers take with respect to man-made disasters and terrorism. It was shown that particular problems make it difficult to insure third party liability for man-made disasters.

One problem is that demand for these types of insurances may be relatively limited, generally due to a preference of industry to externalise harm to society. That, of course, reduces incentives to seek insurance coverage for which premiums would have to be paid. The remedy suggested in the literature is to impose mandatory liability insurance. A few cases we presented from the Netherlands showed that this may be necessary. However, for a variety of reasons, one can notice a large reluctance on the side of policy-makers to introduce mandatory guarantees, as was also already clear from the legal analysis in Chapters 3 and 4.

The main problem in insurance of third party liability for man-made disasters and terrorism may be related to supply-side problems which cause a reluctance on the side of insurers to engage in the coverage of these types of risks. The highly correlated nature of catastrophic risks, the high capacity needed for these high damage events, lack of predictability and statistics all make man-made disasters and terrorism “difficult to insure”. The answer to that problem given not only in literature, but also in practice, is a role for government to facilitate insurability in different capacities. It often takes the form of government acting as reinsurer of last resort.

Some examples, such as the case of the nuclear liability conventions show that government merely provides an additional layer of financing and, in fact, does not stimulate insurability. Case studies related to terrorism, but also to Fukushima showed that there are examples where government can play a positive facilitative role in stimulating insurability of man-made disasters and terrorism. For example, the Spanish CCS charges a premium in exchange of the provision of insurance coverage and the same was the case for the indemnity agreement provided by the Japanese government for nuclear accidents. In some cases, like in the TRIA in the US, reinsurance is an outright subsidy, since insurers do not pay a premium for the state intervention provided. The NHT in the Netherlands on the other hand does charge risk-based premiums and moreover creates strong incentives to create market solutions since premiums are set in such a way that it becomes attractive for private (re)insurers to develop their own insurance products.

Of course, an important observation related to the preference for one solution or the other may be related to costs. On the one hand, one will have to take into account the potential costs that may arise in case no solution would exist, as e.g. the case of The Netherlands showed where operators succeeded in externalizing harm. However, these costs of damage externalization will have to be balanced against the potential costs of a mandatory regime. The problem with e.g. mandatory securities is that a mechanism like insurance will always lead to costs that are higher than the objective value of the risk. The reason is that insurance also creates administrative costs (so-called loading) and that insurers make a profit. Especially in cases where operators would not be risk averse (e.g. because they would have substantial assets at their disposition and hence could self-insure) the additional costs of a mandatory regime may be substantial and should hence be taken into account.

The important lesson for the case of the security industry may be that the different schemes and examples we discussed show that even though there are substantial difficulties that insurers face in covering third party liability for man-made disasters and terrorism, insurance techniques have been developed to mitigate those problems as a result of which e.g. terrorism became insurable again after most insurance companies first cancelled their policies after
9/11. Interestingly, government played a facilitative role in stimulating those insurance solutions which may be an interesting example for the security industry as well. Several examples also show that it is possible to construct this government intervention in such a way that it mimics market principles (e.g. by charging a risk-related premium) and hence stimulates the functioning of the (insurance) market, rather than distorting it (as was the case with the nuclear liability conventions discussed in Chapter 5).

6.4. Insurance of natural disasters

In this section we will focus on the approach insurers take towards the coverage of large-scale natural disasters. Like in the case of man-made disaster and terrorism, we discussed in the previous section, it has taken many developments and evolutions in several countries to come to an adequate coverage of natural disasters. The reasons are similar as in the case of man-made disasters and terrorism: there are substantial problems both on the demand-side as well as on the supply-side that explain why these insurances have not emerged on a large scale (with the exception of the countries where insurance has been made compulsory, like in Belgium and France). We will discuss those problems and the solutions insurers have developed, whereby, again, facilitative strategies provided by government have played an important role.

From the outset it should, however, be mentioned that in the case of natural disasters we, in principle, do not address tort law or liability insurance, but first party insurance. The reason is that natural disasters are often deemed “acts of God” or force majeure as a result of which no injurer can be identified which could be held liable. The only possibility to use liability rules in case of a natural disaster is often to focus on public authority liability. Many have argued that there is in fact no such thing as a natural disaster since most catastrophes are produced jointly by nature and humans. Nature creates a flood; what turns the flood into a disaster is for example the decision of government to provide permits for building in flood prone areas. After disasters the only possible liable party would then be a public authority for failure to take adequate preventive measures or to give adequate warnings. The insurance solutions we are hence referring to here are so-called first party insurance schemes which basically amounts to an insurance coverage taken by a potential victim to seek protection against consequences of a natural disaster.

6.4.1. First party insurance for natural disasters

First-party insurance is a system whereby insurance coverage is provided and compensation is awarded directly by the insurer to the victim. It is thus the prospective victim himself who buys this type of insurance coverage, with an eye on possible future harm and corresponding damages. The underlying principle in first-party insurance is that the insurance company – in principle – pays as soon as damage occurs, provided that it can be proven that the particular damage is an insured risk covered by the insurance policy. Contrary to third party insurance, payment by the insurance company occurs irrespective of whether there is liability.

Accordingly, insurance protection trends away from tort law and third party insurance and towards insurance schemes whereby victims ex ante seek coverage on a first-party basis where possible. For example, in the area of environmental insurance there is a movement

---

734 This corresponds to Task 4.4 of Work Package 4.
735 See Zeckhauser 1996, p. 113.
736 See on the governmental responsibility after Katrina Bier 2006 and Walter and Kettl 2006.
737 Faure and Hartlief 2003. See also on the difference between first party and third party insurance supra 6.1.3.
toward environmental damage insurance operating as a form of first party insurance.\textsuperscript{738} There is a similar movement toward first-party insurance in some legal systems in medical malpractice insurance\textsuperscript{739} and when compensating traffic accident victims.\textsuperscript{740} The benefits of various first-party insurance schemes are accordingly being used to address a range of societal issues. Indeed, Priest suggested that the shift towards first-party insurance would have been an appropriate remedy to the American insurance crisis that occurred in the eighties.\textsuperscript{741} Priest reasoned that:

\begin{quote}
[In comparison to first-party insurance, third party tort law insurance provides coverage in excessive amounts, in a manner that substantially restricts risk segregation, and at costs that far exceed the costs of first-party insurance. For both consumer and provider risk pools, these differences will increase the correlation of risks within existing pools and, as a consequence, increase the extent of adverse selection, leading to the breakdown of the pools.\textsuperscript{742}]
\end{quote}

Other commentators, such as Bishop and Epstein, also favour first-party insurance.\textsuperscript{743} It has particularly been argued that first-party insurance schemes have the advantage of low administrative costs\textsuperscript{744} as well as the ability to better adapt premiums and policy conditions to specific risks.\textsuperscript{745} The latter enables first party insurance to engage in easy risk differentiation, which is advantageous for insurers. Under this arrangement it is possible for the insurer to assess ex ante the risk and consequently damage that a particular victim would suffer.\textsuperscript{746} This ex ante analysis is not available with third party insurance because assessment of risk is to a third party not known at the time of contracting and potential liability that may or may not follow.\textsuperscript{747} Lower administrative costs are due to the fact that under a first-party insurance policy the insurer covers the risk of damage to a particular victim or a particular site.\textsuperscript{748} It is therefore much easier for the insured to signal particular circumstances, which may influence the risk to the insurer.\textsuperscript{749} The reason for the trend away from third party insurance and towards first-party coverage thus becomes clear.

First-party insurances can be divided into two main groups: (1) insurance, which compensates for personal injuries; and (2) insurance, which takes the form of coverage for specific property damage.\textsuperscript{750} The schemes, which focus on personal injury compensation usually, do not vary coverage based on the source of the injury, i.e. whether the cause was a catastrophe or not.\textsuperscript{751} Accordingly, it takes the form of generalized accident insurance coverage. As a result, coverage depends on the specific costs that a victim would incur as a result of an accident, such as lost income, coverage of (additional) medical expenses, and in some cases even pain and suffering.\textsuperscript{752} Most European countries cover a majority of personal injury

\textsuperscript{738} Faure 2002.
\textsuperscript{739} Wendel 2004, p. 367 (showing Swedish system of patient insurance).
\textsuperscript{740} Faure 2001, p. 177-179; Tune 1996.
\textsuperscript{741} Priest 1987, p. 1552.
\textsuperscript{742} Id., p. 1552-1553.
\textsuperscript{743} Bishop 1988; Epstein 1985; Epstein 1996.
\textsuperscript{744} Indeed, one will not spend time nor money looking for a liable tortfeasor and bringing liability claims. Epstein 1996.
\textsuperscript{745} Perry 2004, p. 771-778.
\textsuperscript{746} Bishop 1988, p. 246.
\textsuperscript{747} Epstein 1985, p. 648-650.
\textsuperscript{748} Bishop 1988, p. 249.
\textsuperscript{749} Id.
\textsuperscript{750} Medaglia et al. 1995, p. 829.
\textsuperscript{751} Id. at p. 829-830.
\textsuperscript{752} This is more particularly the case in the French policy referred to as “Garantie contre les accidents de la vie”. This new insurance policy provides broad (first-party) compensation against accidents and compensates as if tort law were applicable, therefore including compensation for pain and suffering. See also The French GAV®
expenses through a social security system. Consequently, well-informed potential victims can purchase additional or complimentary coverage according to their individual degree of risk aversion and corresponding need for insurance.

The second type of first-party insurance schemes applies (only) to property damage, for example housing insurance. In many countries, however, first-party insurance for property damage excludes damages caused by a natural disaster. In the Netherlands, for example, property damage caused by flooding is excluded.

6.4.2. Demand side problems

A first problem is that empirical evidence has demonstrated that even in those countries where disaster insurance is widely available (such as in the US and in Europe), individuals tend not to make sufficient use of it, resulting in dramatic cases of underinsurance. This was shown for example after the “flood of the century” of the river Elbe in Germany as well as in the US, especially after Katrina. Several reasons are indicated for this low demand for disaster insurance. First, as a result of cognitive limitations, low probability events like natural disasters are systematically misjudged resulting in a “it will not happen to me”-attitude. Second, there is equally empirical evidence that people ex ante prefer uncertain losses rather than the certain loss incurred by paying the premium. Insurance is considered an investment. The problem with disaster insurance is that a potential victim (like a house owner) is confronted with the certain loss of a premium, whereas there is a low expectation of a return on the “investment” during a lifetime and hence a low demand. Third, some literature indicates that also ex post government relief (i.e. provided after a disaster) may reduce incentives to purchase insurance coverage.

6.4.3. The case for comprehensive disaster insurance

Given the many problems on the demand side an efficient demand for insurance for natural disasters hence does not emerge. It has therefore been suggested in the literature (in fact since 1968 repeatedly by Kunreuther) that a system of mandatory comprehensive insurance should be created.

6.4.3.1. Theory

The economic rationale behind compulsory (liability) insurance was the externality argument: in the absence of adequate insurance, injurers could (through their insolvency) externalize risk. As was indicated in Section I.A, that may be an argument in favour of compulsory


Miller 1982, p. 554-556.

This assumes that competitive insurance markets offer applicable policies.


See Daniels, Kettl, et al. 2006.


Kunreuther 1996, p. 175.


This is a point strongly made by Epstein 2006; and by Harrington 2000.

Kunreuther 1968.
liability insurance. However, the argument for compulsory liability insurance is not particularly convincing in the case of first-party insurance, where one can argue that victims that are not adequately insured for personal injury can then call extensively on the healthcare system and thus “externalize” that risk. Yet, given that most European legal systems provide (through social security) wide coverage for healthcare (precisely through mandatory healthcare insurances), it is difficult to see why that should be supplemented with an additional compulsory accident insurance. The same is true for the property damage that victims may suffer as a result of a (natural) disaster. While the absence of insurance may lead to additional calls from victims on government relief (and as a result of political pressure caused through a large number involved they may succeed), there is no direct issue of externalization of their harm.

The second traditional economic argument in favour of compulsory insurance is that of information problems. This assumes that citizens are not averse to the risk of large damage as a consequence of catastrophes, and would be willing to pay a premium to have that risk removed from them, but simply do not purchase insurance because they lack information on the probability and magnitude of the risk and/or on the availability of insurance. Given the result of psychological experiments, it could be argued that because of imperfect information, individuals are not fully informed about their own preferences. Regulation would then be the classic remedy to cure an information deficiency.

This could constitute an argument in favour of compulsory (first-party) insurance for property damage caused by natural disasters, where empirical evidence showed that victims greatly underestimated these risks and would, being well informed, demand insurance. Or one could take into account the results of happiness research and argue that people might experience higher life satisfaction or subjective well-being if ex ante arrangements guaranteeing financial compensation after disasters could be made. Support for a regulatory duty to insure against disasters, in addition to voluntary housing insurances (such as is the case in France), can also be drawn from behavioural experiments that show that where disaster insurance is sold along with insurance against likely losses (like housing insurance) at a reasonable extra cost, this will lead to more people taking out insurance against low-probability loss. Thus, this literature concludes that if it is in society’s best interest for people to insure themselves against unlikely calamities, then adding protection against a small but likely loss might help accomplish this purpose.

There are, however, drawbacks to such a duty: first, the limited empirical evidence available showed that it is not only the lack of information on risk that causes the low demand for insurance, but rather bounded rationality linked to the idea that “it will not happen to me”, combined with the unwillingness to pay a premium for an unlikely hazard. The question thus arises whether forcing people to take out disaster coverage should not be considered as paternalistic.

Second, if, on the contrary, one assumes that potential victims are poorly informed as to their potential exposure to disasters and the benefits of first-party insurance, regulatory intervention should instead focus on mandatory disclosure of such information to potential victims rather

764 See generally Schwartz and Wilde 1979.
765 Kunreuther 1968.
767 See Slovic et al. 2000, p. 60-61 and 70-71. It is equally held that compulsory insurance is a good example of a policy that can play a role in improving hazard perception (Slovic, Kunreuther and White 2000, p. 25).
768 Kunreuther 1996, p. 175.
than mandatory coverage. Again, this is supported by behavioural experiments, which show that graphic presentations may - to some extent - increase the perceived risk of that hazard.\textsuperscript{769}

Third, if a duty to purchase “disaster coverage” were to be introduced for all victims, those who do not run any risk may be at a disadvantage. Taking the example of flood insurance, one can imagine that a person living in a house close to a river might desire flood insurance, where someone living in a twentieth-floor apartment far from a river will not. A generalized duty to purchase insurance coverage would therefore force all individuals to take insurance coverage, even where they run no risk at all. This could thus create inefficiencies and lead to a cross subsidization, whereby those who run no risk contribute to the premiums of those who may actually benefit from the insurance coverage. A more efficient (and fairer) solution may therefore be that compulsory coverage (e.g., for flood risks) is limited to those individuals who actually are exposed to the particular risk.

It is sometimes held that compulsory insurance for disasters may be necessary to avoid the risk of adverse selection, meaning that only the bad risks would purchase insurance coverage. Thus, it has been held that in order to make the risk insurable, good risks should also be covered and thus disaster insurance (for instance, for flooding) should be made compulsory.\textsuperscript{770} This is indeed a crucial issue that merits some further attention in relation to the insurability of the disaster risk. The remedy against adverse selection is, of course, a pooling of risks, whereby the insurer should have both good and bad risks.\textsuperscript{771} However, it seems wrong to suggest that disaster risk is only insurable if everyone, even those who run no risk at all, is forced to purchase insurance coverage. Adverse selection can also be avoided if only those who are exposed to the risk are forced to take the mandatory coverage.\textsuperscript{772} Within the group that is actually exposed to risk (and presumably has a demand for insurance), an adequate differentiation of risks and premiums, as a remedy to adverse selection, is possible.

Fourth, economists always warn that introducing a duty to insure may be efficient only if sufficient competition on the particular insurance market exists. Where this is not the case, the introduction of a duty to insure creates a dependency, as a result of which the (concentrated) insurance market can de facto decide the conditions at which to sell its product. Obviously, in a monopolistic market compulsory insurance will create inefficiencies.\textsuperscript{773} Further, even if mandatory coverage is introduced, sufficient room should be left for competition. Hence, the additional premium for the disaster coverage should not be fixed by law but should be the result of competition in this respect between insurers.

Fifth, some particular catastrophic risks may be so “new” that insurance markets may not yet have developed an insurance to cover them. If a differentiated supply of insurance policies is limited, one could again question whether it makes sense to introduce mandatory insurance, if such coverage could only be found to a limited extent (or without sufficient competition) on private insurance markets.

Recently Viscusi has also supported the idea of a mandatory disaster insurance. He more particularly defends this approach from the point of view that politicians are unable to deny

\textsuperscript{769} Slovic, Kunreuther and White 2000, p. 15; Slovic 2000, p. 70-71.  
\textsuperscript{770} This argument was, for instance, advanced in the Netherlands by the Dutch Insurers Association with respect to flood insurance. For details, see Faure and Hartlief 2002, p. 183-189.  
\textsuperscript{771} Schwarze and Wagner 2004.  
\textsuperscript{773} It has, for instance, in relation to environmental insurance, also been indicated that if one makes the availability of insurance coverage a prerequisite for the operation of an enterprise, insurance undertakings become the de facto licensors of the industry. This may be particularly problematic from a policy perspective if this happens on concentrated insurance markets (see Monti 2001, p. 65).
Comprehensive insurance may be an attractive alternative. This would at least foster self-protection and insurance.

6.4.3.2. Examples

The most well-known example of mandatory first-party insurance is probably the French model, according to which all individuals who have taken out first-party property damage insurance policies have to pay a supplementary premium for a mandatory coverage for natural disasters. Thus, France does not have a generalized duty to insure but a compulsory complementary coverage on (voluntary) property damage contracts. However, those property damage policies are widespread, and all individuals who purchase such a policy have to pay for the additional coverage for natural disasters. This system is apparently accepted in France, because the risk of cross-subsidization may be small: France seems to be confronted with many types of natural disasters. This means that if one is (as inhabitant of an apartment on the twelfth floor) not exposed to the risk of flooding, one may be at risk from other natural disasters, such as earthquakes or heavy storms.

Belgium has moved to a similar model: Belgium has had a compensation fund for disasters since 1976; as a result of a legislative change in May 2003, a compulsory flood coverage has been introduced in addition to the voluntary property damage insurance contracts. The Belgian model appears at first to ape the French system, but the major difference is that this mandatory supplementary coverage applies only for specific risk areas. This thus avoids a negative redistribution, as those who are not exposed to the risk are not forced to take out the coverage. Recently, this system was again changed, and Belgium now follows the French model of mandatory disaster coverage. In Belgium the disaster coverage applies to voluntary fire insurances. Belgium now follows the French model of mandatory disaster coverage.

In Italy and Germany, legislative initiatives looking at some form of mandatory coverage against damage caused by disasters are currently under discussion.

Note, moreover, that in France, as a result of the explosion in Toulouse on 21 September 2001, a legislative change was enacted in July 2003 that ensures that victims now also have additional compulsory coverage for damage caused by technological risks (such as the explosion in Toulouse). The benefit of this change is, however, debated (also in France). It is not so clear why a mandatory coverage for victims was introduced for technological disasters.

---

774 Viscusi 2010, p. 142-148. He argues “Saying that one will not support assistance after a future hurricane may, of course, be a form of hypothetical trash talk. It is a quite different matter to actually deny assistance once there are identified victims with their stories featured on the evening news” (p. 146).

775 As also held by Kunreuther and Pauly 2005.


777 The supplementary coverage for disasters is financed through an additional premium of 12 percent on all property damage insurance contracts. See, for a description and critical analysis of this French model, also Schwarze and Wagner 2004 and Laflay, Cannarsa and Moréteau 2006.

778 The same point is made by Schwarze and Wagner 2004: if previously distinct risks are pooled (like flood, windstorms, and hail), individual exposure to some risk would almost be guaranteed.

779 Through the charging of exposure-related premiums “cross-subsidization” between various areas could be reduced (Schwarze and Wagner 2004).

780 For a critical discussion of the Belgian system, also with a comparison to the Netherlands see Bruggeman 2011 and Faure, Bruggeman and Haritz 2010.

781 Act of 17 September 2005, Moniteur Belge, 11 October 2005. It seemed impossible to pursue the idea of limiting the mandatory coverage given the high (political) costs of identifying the special “risk areas” where the duty to insure would apply.


783 Again it concerns a mandatory supplementary coverage for damage caused by technological disasters on voluntary insurance contracts.
disasters, when a liable wrongdoer can be identified, where the introduction of solvency
guarantees on the side of the wrongdoer, such as compulsory liability insurance, could have
been examined instead.

6.4.4. Supply side problems

Even though it is – as just indicated – questionable whether there is a high demand for
catastrophe insurance, there are definitely problems on the supply side. A number of insurers
exclude coverage for property damage caused by (natural) catastrophes and argue that those
losses are uninsurable. The three principal reasons for this attitude are the fear of catastrophic
losses, the uncertainty of the risk, and the lack of insurance capacity. 784

First, natural hazards normally occur within one specified area and are highly correlative. Past
disasters indicate that a significant number of (especially non-geographically diverse)
insurance companies became insolvent as a result of such catastrophic losses. Consequently,
property insurance became increasingly difficult to obtain in hazard-prone areas.

Second, the absence of historical data and the present imperfect scientific knowledge
contributes to the supply deficiencies of first party catastrophe coverage. 785 However, this
point needs to put into perspective due to the new insights into catastrophe modelling. 786 The
lack of predictability regarding both the probability of an extreme event occurring and of the
outcomes of such an event results in ambiguity. This ambiguity may lead to uninsurability of
a specific catastrophic event or in a specific hazard-prone area. 787 Insurers can, however, take
account of this uncertainty regarding the probability of catastrophic damage by charging a so-
called risk premium. 788 Nevertheless, two problems still exist: (1) a higher insurance premium
can in turn decrease demand for insurance against catastrophic risks; and (2) insurance
regulation might limit insurers’ ability to apply high premiums to catastrophic risks. 789
Regulated rates are in fact a major problem in some countries and may be, in certain high-risk
areas, the main obstacle to an effective voluntary insurance market for consumers. 790

Third, insurance companies need sufficient financial reserves to cover the particular
catastrophic risk. 791 In many cases, however, and especially with catastrophic events, the
expected loss may exceed the capacity of the individual insurer.

Moreover, pooling between insurers may in some cases lead to welfare losses as a result of
cartel agreements that de facto cause the uninsurability of natural disasters.

For example, in the Netherlands during the 1950s, the Dutch Insurers’ Association issued a
so-called “binding decision” on all of its members, prohibiting them from insuring flood and

785 See Faure and Hartlief 2003.
786 See generally, Hartington et al. (1997) (Discussing scientific issues associated with catastrophes).
788 Kunreuther et al. 1995, p. 338. Doherty et al. recently found that, under a 1-year contract, mean annual
premiums are 25 percent higher when the probability of the event is ambiguous than when it is given precisely.
Under the 20-year contract, aversion to ambiguity is even stronger. See Doherty et al. 2008. p. 147. The source of
the uncertainty does not affect the insurers, contrary to Cabantous’ beliefs. Cabantous 2007, p. 220, 235.
789 Faure and Hartlief 2003, p. 83,86.
791 Doherty accurately draws the attention upon the fact that the importance of capital as a requisite to secure an
adequate rate of return is often not fully understood. After all, the capital needed by the insurance firm to be able to
cope with catastrophic losses must be high enough to cover 1) the expected claims costs and other expenses, and 2) the
costs of allocating risk capital to underwrite this risk. See Doherty 2008, p. 149.
earthquake risks (the latter being a relatively small risk in the Netherlands with the exception of the area around Southern Limburg). Their argument was that these risks were technically not insurable since the flooding and earthquake risks were uncertain in their nature and hence, difficult to calculate. Moreover, these types of insurance would only be attractive to high-risk individuals (e.g. those living in flood prone areas) and this would result in incurable adverse selection. As a consequence, it was determined that the members of the Dutch Insurers’ Association should all refrain from covering these risks.

The arguments concerning the uninsurability seemed highly doubtful, but the Association’s binding decisions also clearly violated competition law. At the time European Commission Regulation 3932/92 of December 21, 1992 exempted many cartel agreements in the insurance world from the prohibition under the old article 85(3) of the EC Treaty. The Regulation provided that certain strict conditions were met. Law and economics scholars, who argued that competition policy should be fully applied to insurance markets, heavily criticized this exemption. The binding decisions not to insure flood and earthquake risks not only clearly limited supply (it effectively excludes it as a result of a cartel agreement), but it also violated the conditions of Regulation 3932/92. Consideration 8 preceding the Regulation, states that standard policy conditions may not contain any systematic exclusion of specific types of risk without providing for the express possibility of including that coverage by agreement. This is repeated in article 7(1)(a) of the exemption. The European Commission also issued a report to the European Parliament and to the Council on May 12, 1999 concerning the functioning of the exemption in Regulation No. 3932/92. In this report, the Commission explicitly discusses these binding decisions. The report states that as a result of the questions asked by the Commission, the Dutch Association of Insurers decided to bring its binding decision in line with Article 7.1, Subsection a, by simply converting it into a non-binding recommendation, which left each insurer free to extend coverage to flood risks. This example demonstrates that a minimal supply of insurance coverage may well be the result of anti-competitive behaviour by insurers, who mutually agree not to cover particular catastrophic risks.

At a policy level, this demonstrates that a necessary condition of insuring catastrophic risks is a competitive insurance market that offers a wide variety of differentiated insurance policies and responds to the demand of the market. Instead of direct government intervention, government should guarantee an adequate competition policy with respect to insurance

---

793 Pursuant to old Article 85 (3) of the EC Treaty, agreements, decisions by associations of undertakings and concerted practices in the insurance sector which seek cooperation with respect to: (a) the establishment of common risk-premium tariffs based on collectively ascertained statistics or on the number of claims; (b) the establishment of standard policy conditions; (c) the common coverage of certain types of risks; or (d) the establishment of common rules on the testing and acceptance of security devices, shall not be prohibited as incompatible with the common market. EC Treaty Article 85 (as in effect 1985) (now article 81), available at <http://ec.europa.eu/comm/competition/legislation/treaties/ec/art81_en.html> (last visited October 22, 2008).
795 Consideration 8: Standard policy conditions may in particular not contain any systematic exclusion of specific types of risk without providing for the express possibility of including that cover by agreement and may not provide for the contractual relationship with the policyholder to be maintained for an excessive period or go beyond the initial object to the policy. This is without prejudice to obligations arising from Community or national law. 1992 OJ (L 398) 7-14, available at <http://eur-lex.europa.eu/RECH_celex.do> (enter Cylex number 31992R3932) (last visited October 22, 2008).
796 Report from the Commission to the Council and the European Parliament on the operation of Commission Regulation No 3932/92 concerning the application of Article 81 (ex-Article 85), paragraph 3, of the Treaty to certain categories of agreements, decisions and concerted practices in the field of insurance, COM 1999, 192 final.
markets. Otherwise uninsurability may, as the Dutch example shows, simply be the result of a cartel agreement.  

Therefore, as long as insurers are able to estimate the frequency and magnitude of potential catastrophic losses, catastrophic first-party insurance is and should be available. Due to problems of ambiguity, adverse selection, moral hazard, and highly correlated losses, insurance companies will want to charge a risk premium that considerably exceeds the expected loss. This premium can, however, be so high that there would be very little demand for coverage at that rate. In such cases, the insurer will not want to invest the time and money necessary to develop the product. If the insurer is convinced that there is sufficient demand, he will try to raise sufficient capacity to survive possible catastrophic losses.

6.4.5. Government support needed?

Like in the case of man-made disasters and terrorism which we discussed in the previous section, here we can also suggest that a facilitative strategy whereby government would act as reinsurer of last resort may at least cure of some of the supply side problems in the insurance of natural hazards. Since the theoretical and policy considerations behind facilitative strategies by government to stimulate insurability have been explained in the previous section we can now suffice with providing a few examples of insurer approaches towards large-scale natural disasters with government support.

6.4.5.1. CCR

France installed a publicly owned reinsurance company, the Caisse Centrale de Réassurance or “CCR”. Reinsurance is not compulsory, and insurers are free to contract with other, private, reinsurance companies. Reinsurance with the State reinsurance company is, however, particularly attractive, both because of the reinsurance premiums it charges and because it can offer unlimited cover since it can benefit from a State guarantee in the event that the CCR exhausts its resources. However, a CCR official noted that insurance companies must transfer half of their (natural) catastrophe risk to the CCR in order to be covered under the State guarantee. The State thus intervenes as a reinsurer, or, more correctly, as a retrocessionaire of the CCR. In exchange for this State guarantee, the CCR pays a premium to the State (Article R. 431-16-2 Insurance Code), exactly as it should have done if it was protecting itself through an ordinary reinsurer, although evidently the latter could not have delivered him an unlimited guarantee. The reinsurance program is set up so that insurers manage

797 We do not argue, however, that competition necessarily provides better results than (state) monopolies. See Winand Emons 2001, p. 247-248 (empirical researched showed that under specific circumstances, particularly when insurers are unable to differentiate risks adequately, a natural monopoly with one (state) insurer may provide better results than a competitive environment); see also Von Ungern-Sternberg 1996.

798 Government acting as reinsurer of last resort can of course only deal with the first mentioned supply side problems of correlation, uncertainty and limited capacity but not remedy the kartel agreement not to cover particular risks. In that case competition policy should provide a remedy as it did in the case of the Netherlands (even though there is still only limited flooding insurance available in the Netherlands).

799 See supra 6.4.4.


801 GAO 2005, p. 33.

802 Bidan 2001.
policyholders’ claims because they have the best claims-paying experience and expertise. Coverage from the CCR takes effect after insureds pay a certain deductible.\footnote{CCR’s coverage for natural disasters is unlimited because of the State guarantee. The deductible under the CCR reinsurance contract, therefore, represents the maximum amount that an insurer will have to bear in the course of a year, regardless of how many losses occur.}

Insurance companies that decide to reinsure with the public reinsurer are offered two types of contracts: quota-share contracts and stop-loss contracts. With a quota-share contract, the insurer cedes a certain proportion of the collected premiums to the reinsurer and the reinsurer undertakes, in return, to pay the same proportion of the losses. The reinsurer will then truly follow the fortunes of the insurer, since the latter has to cede a percentage of each of the policies in its portfolio to the reinsurer. The adverse selection risk is hereby avoided. The proportional cover could vary between 40\% and 90\%. On the other hand, with a stop-loss contract, the reinsurance company covers all claims that exceed an agreed multiple of annual premium income. The insurer will then be protected against the risk of many claims occurring. In order to avoid that insurers bought their risk-sharing cover from private reinsurers and used the CCR only for stop-loss cover, the two contracts were tied: stop-loss contracts were only offered to those insurance companies who also bought quota-share contracts from the CCR with a minimum participation of 40\%. Jametti and von Ungern-Sternberg hereby conclude that the combination of these two types of reinsurance necessarily implies that the CCR (and ultimately the tax-payer) will bear most of the cost when a large-scale disaster occurs.\footnote{Jametti and von Ungern-Sternberg 2004.}

In the first 20 years of its existence, the CCR never managed to accumulate any substantial level of reserves, despite the fact that the average claims/premium ratio of disaster insurance since its creation was only 60\%. Nevertheless, only very few changes to the reinsurance scheme were made, although the CCR reinsured mainly the bad risks\footnote{See: von Ungern-Sternberg 2007, p. 160, at p. 86-95. Since the insurers have the right, but not an obligation, to reinsure a share of their natural disaster risk with the CCR, they have a strong incentive to lobby the government to set high premiums for natural disasters. It is then in the insurers’ interest to reinsure only a small part of their risks and keep the rest of the premiums for themselves.} and excessively high compensation (24\%) was paid for (largely imaginary) administrative costs.\footnote{The effective cost of disaster insurance for the private insurers were, of course, almost nil, since disaster insurance was simply added to already existing property insurance contracts. In comparison, Spain, which is having an identical system of premium collection, only has a 5\% commission for administrative costs.} In addition, the combined effects of changes in the market (mergers, freedom of services within Europe, etc.) and the deterioration of the claims figures made it increasingly unsuitable for just a single scheme to be offered. As a result, from 1 January 1997 onwards, the CCR introduced new reinsurance conditions which paid greater attention to the nature of each ceding company’s portfolio and enabled insurers to retain a larger proportion of the risks.\footnote{CCR 2007.} Still, the \textit{Caisse Centrale de Réassurance} was in 1999 on the verge of bankruptcy after it was called upon to make a major withdrawal on its reserves. Indeed, although no exceptionally large event occurred in 1999, two major events hit France: the flooding in the Aude department in the south during November 1999 (insured losses of € 240 million) and a flooding following the winter storms Lothar and Martin (insured losses of € 240 million). A significant hurricane also occurred in the French Antilles the same year. At the same time, an unexpected peril new to the industry and to the scheme which appeared in 1989 – namely subsidence – had induced the erosion of CCR’s reserves over time. The State guarantee was consequently called into play. As a result, other amendments to the reinsurance scheme needed to be made with the aim of better adapting to the market situation and loss record by e.g. modifying the underwriting conditions, changing the applied deductibles, changing the deductibles in case...
the municipality does not have a PPRN, recapitalizing its reserves (the government injected 3 billion French francs, or € 460 million), abolishing compensation for administrative costs, etc.

Von Ungern-Sternberg, amongst others, hereby concludes that these various amendments to the CCR scheme are the outcomes of flaws in the institutional setup. Cannarsa and others, backed up by the Insurance Journal and A.M. Best, on the other hand, attribute a very positive outlook to the CCR.

6.4.5.2. CEA

The California Earthquake Authority (“CEA”) provides an example of a government stepping into the private insurance market and assuming the risk of a potential natural catastrophe. In short, the California Earthquake Authority is a publicly managed, privately funded organization (without government backing) that was established in September 1996, after the Northridge earthquake in 1994, by the State of California to sell California residential earthquake insurance policies through participating insurance companies and to encourage Californians to reduce their risk of earthquake losses.

The State of California requires insurers doing business in the State to offer also earthquake coverage in their homeowners’ policies, either directly or through a separately State-sponsored earthquake fund, the California Earthquake Authority. The CEA is empowered to set premiums and to bear risks, but a so-called “mini-policy” lays down which classes of real estate losses are covered and which not. In addition, the premiums must be set on an actuarial basis, but, in practice, the quoted CEA premiums have been tempered so that the price differences between the regions are moderated. Also, the CEA may purchase reinsurance, but it does not have access to public funds. As a result, CEA resources are only adequate to compensate an event which is double the size of the Northridge Earthquake, but beyond that level, policyholders will only receive partial compensation.

Participation in the California Earthquake Authority is voluntary, so that private insurance companies may and do compete with the CEA, although this competition is mainly limited to the low-risk locations. It seems that the CEA charges considerable premiums and many homeowners find these too high relative to the coverage provided. Consequently, the percentage of Californians with earthquake coverage (through CEA or a private insurer) declined from 33% in 1996 to 12% in 2010. The Authority currently has a claims-paying capacity that exceeds $9 billion and writes 70% of earthquake premiums. The CEA provides for deductibles of 15 or 10%. These rather high deductibles are subject to criticism. Further the CEA is criticized for its low compensation amounts.

References:

808 The PPRN is the Plan for the Prevention of Foreseeable Natural Risks (Plan de Prévention des Risques Naturels Prévisibles) and is a specific plan that municipalities have to draw up concerning the prevention of catastrophic risks.


811 See Moréteau and Cannarsa 2006, p. 102.

6.4.6. Conclusions Natural Disasters

The concluding observations at the end of this section are similar to those presented in the previous section. We noticed that the insurer approach towards large-scale natural disasters is also largely influenced by problems with covering natural disasters both on the demand side and on the supply side. Empirical evidence showed that notwithstanding large subsidies on insurance for natural disasters (for example, in the case of flooding insurance provided by the National Flood Insurance Plan in the US) insurance coverage is relatively low. Many behavioural phenomena explain why demand remains lower than efficient. The answer provided by insurance specialists is to impose mandatory coverage for natural disasters. The typical example is the one of France, recently followed by Belgium and advocated by scholars in other European countries and in the US as well. This may be the only approach to guarantee large-scale coverage against natural disasters.

Like in the case of man-made disasters and terrorism problems on the supply side have been remedied through intervention of the government as reinsurer of last resort. Again, it can be questioned whether those interventions are examples of efficient government strategies. For example in the case of the CEA government steps in as primary insurer and thus competes with other insurers. Also the CCR in France does not stimulate the emergence of a market solution and neither the CEA nor the CCR seem to have a temporary character.

Many other examples exist of government intervention as reinsurer of last resort in the areas of natural disasters and terrorism. E.g. in Germany (like in most other European Member States) terrorism insurance is provided via a pool in which government also participates, referred to as Extremus. The model is always similar: after a first layer being provided by insurers and a second by reinsurers, a third layer (of which the amount can depend upon the specific Member State) will be provided by government. As we mentioned, although there may be certain advantages in those schemes (more particularly of still providing insurance coverage where market supply would otherwise fail) there are certainly disadvantages as well, which depend on the specific construction chosen. One problem is that if government provides reinsurance without charging a price, this amounts to an outright subsidy which may provide perverse incentives to operators and will have the result that risks are not accurately reflected in prices. Moreover, to the extent that government provides the third layer of compensation for free, it are in fact tax payers that provide compensation to the benefit of victims. To that extent, one could argue that potential victims pay for their compensation themselves instead of those who are creating the risk. However, in some Member States (like in The Netherlands) the third layer is not provided for free by government but government charges a price which should precisely provide incentives to the market players to reduce the government intervention as much as possible. This has, e.g. in The Netherlands, had the desirable effect of reducing the government intervention in the third layer overtime.

However, the important point to remember from those examples is the trend towards public private partnerships whereby government intervenes in a facilitative strategy to stimulate insurability of catastrophes, in this particular case natural disasters.

6.5. Conclusions chapter 6

---

813 Interview with representatives of a large reinsurance company on 12 March 2013.
814 For a further and more detailed discussion of the advantages and disadvantages of the intervention of government as reinsurer of last resort with a discussion of examples see Bruggeman, Faure and Heldt (2012) 185-241.
6.5.1. Relevance for the security industry

Within the scope of this chapter, we first discussed contractual practices by other industries regarding third party liability risk limitations. More particularly, we discussed the software industry, the pharmaceutical industry and the meteorological industry.

The experiences from these other practices and sectors are to some extent useful, in the sense that also for the case of the security industry contractual limitations of liability could play an important role. Of course, whether partners will accept these types of limitations will depend on the question of the specific market structure and bargaining power of both parties. Also, the discussion of these three other sectors showed that the respective strength and weaknesses of each approach were very much dependent upon the specific industry. The experience in other industries shows that other industries are to some extent able to hedge their liability risks via insurance and contractual arrangements. These are obviously constructions that the security industry could try as well. However, on the basis of an analysis of the meteorological, software and pharmaceutical industry, it is of course not possible to predict to what extent the security industry would be able to obtain similar risk limitations as those other industries did.

The discussion of man-made disasters and terrorism showed particular supply side and demand side problems. On the demand side, it was argued that for some man-made disasters demand for insurance is simply too low as a result of which an externalization may take place. That may hence constitute an argument in favour of mandatory insurance. Interesting for the liability exposure of the security industry is especially the fact that for terrorism private-public partnerships have been developed, whereby the government provides a role as reinsurer of last resort. This shows on the one hand that the insurance may have been developed to mitigate problems of insurability; on the other hand, it also shows that e.g. terrorism risks for operators are, as a result of these regulatory interventions, now largely insurable. That may hence reduce the need to call on the security industry and thus the liability exposure of the security industry.

Although the case of natural disasters is probably less directly relevant for the security industry, it is important to note that also as far as natural disasters are concerned, some solutions have been worked out where the government has intervened as reinsurer of last resort in order to stimulate insurability.

6.5.2. Lessons for a Future Liability Regime for the EU Security Industry

The description of industry practices in the pharmaceutical, software and meteorological industries showed a few interesting features that may be of relevance for a future liability regime. One important point is that in contracts, liability caps are often built in. Such a liability cap can obviously limit the liability exposure of the security industry. To the extent this is possible, the security industry could obviously also negotiate liability caps with their clients (operators) like this is the case with the software industry.

Another interesting feature is that in some legal systems mandatory insurance schemes have been introduced, e.g. in Germany as far as pharmaceutical products are concerned. Such a mandatory liability insurance can on the one hand provide protection to potential victims, but on the other hand also to the security industry. Moreover, again, in the German Drug Act liability is also statutorily capped.

As far as man-made disasters and terrorism is concerned, the argument was made that compulsory liability insurance could be provided in order to avoid an externalization of harm. Such a mandatory insurance would normally in the first place apply to operators, but still the
question could be asked whether mandatory insurance should apply to the security providers themselves as well.

Interestingly, both as far as man-made disasters, terrorism and natural disasters are concerned, as we just mentioned, public-private partnerships have been worked out whereby in some cases government acts as reinsurer of last resort in order to increase insurance capacity. In some cases, as the comparative analysis shows, this has even led to the creation of some fund solutions for terrorism, but also to the creation of specific facilities to provide coverage for terrorism as well. To the extent that those mechanisms are sufficient to provide coverage for terrorism related risks, there is no specific need for further intervention at a legislative level, given the fact that more particularly terrorism related risks constitute the major worry for the security industry.

815 See supra chapter 4.
Chapter 7 The US SAFETY Act

This section covers the legal analysis of the US “Support Anti-terrorism by Fostering Effective Technologies Act of 2002” (commonly known as “the SAFETY Act”). The SAFETY Act was passed by the US Congress as part of the Homeland Security Act of 2002 (“HSA”), Public Law 107-296, to encourage the innovation and introduction of anti-terrorist security products and services after the September 11, 2001 (“9/11”) attacks on the World Trade Center in New York City and other targets in the US. The HSA also established the Department of Homeland Security (“DHS” or “the Department”), a Cabinet-level department within the US government, headed by the Secretary of Homeland Security (“the Secretary”), to administer the new legislation, including the SAFETY Act provisions. As discussed below, the SAFETY Act is the main legal instrument for producers of security-related products and services to limit third party liability claims against them for harms occurring in the US.

The legal analysis of the SAFETY Act covers a range of issues, including:

- an assessment of the legal consequences, including the advantages and disadvantages, of the protections available under the Act;
- an analysis of US cases, i.e. court opinions, involving the liability for providers and users of anti-terrorism security technology, products and services which impacted Congressional action on the Act;
- the position of European security companies in securing protection under the US SAFETY Act; and
- an assessment of the necessary preconditions for the adoption of a EU version of the SAFETY Act as a regulation under European law.

The Work Package includes four tasks. Task 5.1 involves an analysis of the content of the US SAFETY Act. Task 5.2 requires an analysis of existing US case law regarding third party liability of security companies. Task 5.3 addresses the potential of the US SAFETY Act to shield European security companies against limitless third party liability. Task 5.4 provides an analysis of the necessary EU framework preconditions for enacting a similar legal act.

7.1. Legal analysis of US SAFETY Act

This section provides a general overview of the US SAFETY Act (“the Act”) including (a) its background, rationale, and implementation; (b) liability protections available under the Act; (c) eligibility for SAFETY Act protections; (d) criteria used by the US government for granting these statutory protections; (e) forms and extent of protection available (Designation and Certification); (f) insurance requirement and liability limit for successful applicants; (g) the application process and timeline; and (h) an assessment of the effectiveness, and advantages and disadvantages of the Safety Act protections.

---

816 This corresponds to Work Package 5 of the Invitation to Tender.
818 Congress created the DHS Science and Technology (“S&T”) Directorate as part of the HSA, to “conduct basic and applied research, development, demonstration, and testing and evaluation activities relevant to any or all elements of the Department.” 6 U.S.C. § 182(4). The Office of Public Private Partnerships (“PPL”) SAFETY Act Office is situated within the S&T Directorate and is responsible for reviewing and providing advice to the Secretary related to SAFETY Act applications.
Believing “that technological innovation is the Nation’s front-line defense against the terrorist threat,” the US government wanted to stimulate innovation, development and deployment of anti-terrorism products and services after the 9/11 attacks. However, Congress understood that risk and litigation management issues, derived from the nation’s product liability system and the associated potential liability exposure of manufacturers and users of anti-terrorism products and services, which could lead to potentially crippling litigation, as well as public relations and shareholder issues in the aftermath of a terrorist attack or incident that resulted in litigation, were factors seriously threatening to keep new products and services from the market. Congress also recognized that, adequate and affordable insurance was “largely unattainable or so costly as to leave the technologies in question without a market” to mitigate the types of potentially massive and uncertain liabilities for hopeful developers and providers of anti-terrorism products and services stemming from lawsuits that could be brought against these companies by victims of terrorist attacks. As a result, Congress found it “hardly surprising that companies are unwilling to bet their existence by developing and deploying services and products in this uncertain climate.”

Moreover, before the Safety Act was enacted in the US, government contractors became increasingly unwilling to accept the potentially enterprise-threatening risk of developing and deploying anti-terrorism technologies and bidding for related contracts. This self-screening due to liability not only negatively affects the contractors but commercial and government customers as well. It limits the pool of otherwise-qualified bidders, reducing competition and choice of cost-effective best-value solutions for the buyer. Also, as mentioned above, self-screening opportunities based on liability results in a disincentive for industry to invest in security technologies in those areas, leading to a reduction or elimination of investments and a corresponding loss of innovation and technology readiness for deployment. Indeed industry found itself declining to pursue business opportunities because of liability concerns.

The SAFETY Act was intended to encourage the development and deployment of anti-terrorism products and services. It does this by limiting the liability of sellers of these products and services for third-party claims arising out of an act of terrorism where the product or service has been deployed to prevent, respond to, or recover from such an act and capping their insurance requirements. Although it did not have unanimous support, the SAFETY Act passed narrowly.

819 See P.L. 107-296, House R. 107-609 (Part 1) at 118.
820 See Congressional Hearing Before the Subcommittee on Cybersecurity Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives, 112th Cong., First Sess., (statement of US Representative Daniel Lungren (R-CA)) (May 26, 2011) (“Lungren Statement”) (“[[legal precedents such as those emanating from the 9/11 attacks as well as those holding the Port Authority of New York and New Jersey liable for the 1993 World Trade Center attacks make it clear that civil litigation can intimidate the developers and users of security technologies and services after a terrorist event.”)."
822 Id.
823 Stakeholder response to Questionnaire in Annex II.
824 In opposing passage of the SAFETY Act, Senator Joseph Lieberman (D-Mass.) argued that the legislation would give “protection even to those sellers who knowingly put anti-terrorism products on the market that they know won’t work to keep people safe against an attack.” 148 Cong. Rec. S11362 (Nov. 19, 2002). And, even after its passage, Senators Lieberman and Tom Daschle (D-SD) introduced legislation to strike the SAFETY Act provisions from the Homeland Security Act arguing that they “would entitle companies selling that technology to broad liability protection from any claim arising out of ... an act of terrorism, no matter how negligently, or even wantonly and willfully, the company acted.” 149 Cong. Rec. S46 (Jan. 7, 2003). See also Hearing Before the Committee on Government Reform, House of Representatives, 108th Cong., 1st Sess. (Oct. 17, 2003) (Statement of Henry A. Waxman (D-CA) (“This law is not about encouraging innovation, but rather its goal is to limit the legal
In sum, the SAFETY Act affords risk management and litigation management protections for sellers and providers of qualified anti-terrorism technologies and others throughout the supply, distribution, and user chain in the event of an act of terrorism, but the Act does not automatically protect these companies against third party liability. Rather, it authorizes the Secretary to grant an individual company, upon application, the protections available under the Act. It also gives the Secretary broad authority to issue implementing regulations. In 2006, the Secretary exercised this authority, and, after providing notice and an opportunity to interested stakeholders to comment on proposed regulations, promulgated the Act’s final implementing regulations.

7.1.2. Liability protections available under the SAFETY Act

The SAFETY Act employs a number of tools or features to insulate certified security providers against third party liability exposure. Specifically the Act:

- creates a federal cause of action against sellers of anti-terrorism products or services for claims arising out of an act of terrorism when qualified anti-terrorism technologies have been deployed in defense of or response to or recovery from such an act;
- provides exclusive jurisdiction in federal district court for these lawsuits;
- limits the type and scope of relief available to plaintiffs in these lawsuits;
- allows the government contractor defense to absolve some sellers of liability; and
- caps sellers’ liabilities to the amount of insurance coverage determined by the Secretary to be reasonable.

The creation of the specific, federal cause of action makes it clear that the proper respondent in any civil claim is the manufacturer of a security product or the provider of a security service and may that others in the supply chain, including users, contractors, subcontractors, customers, vendors and suppliers, cannot be the target of specific or enjoined litigation and benefit from immunity from litigation in this regard. This is justified on grounds that “[i]f the Seller of the Qualified Anti-Terrorism Technology at issue were not the only defendant, would-be plaintiffs, could in an effort to circumvent the statute, bring claims...against arguably less culpable persons.” This targeting of liability not only simplified the application of the Regulations, and ensures circumvention is not possible, but also creates confidence among suppliers and consumers in engaging in trade and contractual relations with producers and providers for QATTs.

liability of the defense contractors and other manufacturers of antiterrorism products and, in many circumstances, to give them absolute immunity.”

826 See 6 U.S.C. § 441(c).
828 See 6 U.S.C. § 442(a) and (b).
829 "There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.”
830 See 71 Fed. Reg at 33150.
Prior to the passage of the legislation, such types of suits, not otherwise meeting the criteria for federal court jurisdiction, would likely have been brought in State courts and defendants would not have had the benefit of these significant liability protections. As DHS explains in the implementing regulations, federal suits under the SAFETY Act will likely be decided in accordance with the law of the State where the attack occurred.\textsuperscript{831} It should be noted, however, that the Act does not limit liability for harms caused by anti-terrorism technologies when no “act of terrorism” has occurred, such as in the case of ordinary third party liability claims based on third-party injury through negligence, or other product liability actions.

Another key feature of the SAFETY Act is the limitation it places on the nature, type and scope of damages that plaintiffs may seek in bringing an action against a QATT supplier.\textsuperscript{832} Punitive or exemplary damages, i.e. those going beyond the amount necessary to compensate the plaintiff which are imposed on the respondent as a deterrent or sanction for their behaviour, are available to varying degrees throughout the US. The manner in which they are applied varies, often significantly, by case in accordance with the applicable state laws.\textsuperscript{833} Another aspect then of condensing potential cases into a single cause of action, restricted to Federal Court, is that it allows the Act to ban the award of punitive damages in such cases, which could cause constitutional questions if attempted at state level.\textsuperscript{834} The SAFETY Act thus creates a ban on this form of damages from being awarded.\textsuperscript{835} It is noted that provision for the award of this sort of exemplary ‘quasi-criminal’ damages are not a feature of civil liability systems in the European Union. Prejudgment interests, i.e. interest added as time passes to the award of an original judgment is also disallowed under the Act.\textsuperscript{836}

Further liability limiting features of the SAFETY Act operate through the limitations it places on the award of non-economic damages. Ordinarily available to all plaintiffs in third party liability claims of this nature in the US, the SAFETY Act stipulates that such damages may only be sought where the plaintiff has suffered an actual, physical injury i.e. plaintiffs who have not done so are precluded from seeking damages for pain and suffering, inconvenience, mental anguish, loss of enjoyment of life, loss of consortium, injury to reputation or any other non-pecuniary losses.\textsuperscript{837} The total exposure of security providers is further limited by the collateral source compensation requirements, which will reduce the respondent’s liability where they have collected damages from other sources, including, for example, from insurance.\textsuperscript{838}

The creation of the Government Contractor Defense does not just limit the security provider’s liability but potentially creates a potential defense to any third party liability claim, although this is not available to all QATT providers as discussed further under section 7.1.5.

\begin{itemize}
\item\textsuperscript{831} \textit{71 Fed. Reg.} at 33150.
\item\textsuperscript{832} 6 U.S.C. §442(b)(1) ‘No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.’
\item\textsuperscript{834} Id.
\item\textsuperscript{835} 6 U.S.C. § 442(b)(1).
\item\textsuperscript{836} Id.
\item\textsuperscript{837} 6 U.S.C. §442(b)(2)(A) ‘Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.’
\item\textsuperscript{838} 6 U.S.C. §442(c) ‘Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism that result or may result in loss to the Seller.’
\end{itemize}
One major feature of the liability limiting scheme created by Act is, of course, the imposition of a maximum liability ceiling. \(^{839}\) Upon grant of an application approval by the DHS, the security provider will be furnished with the details of the level and amount of insurance cover which he will be required to take out under the Act. This amount, as determined during the application process, is the maximum liability ceiling for any damages awarded in the wake of a terrorist incident against the QATT provider.\(^ {840}\)

### 7.1.3. Eligibility for SAFETY Act protections

In this section, we discuss what types of products and services DHS is likely to deem eligible for SAFETY Act protection.

Under the SAFETY Act and the Department’s implementing regulations, “Sellers” of so-called “Qualified Anti-terrorism Technologies” (“QATTs”) may be eligible for DHS SAFETY Act approval of their product or service. DHS defines the term “Seller” to mean “any person, firm, or other entity that sells or otherwise provides” a QATT.\(^ {841}\) A QATT is defined to include “any technology designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause.”\(^ {842}\)

The Homeland Security Act of 2002 (which created the SAFETY Act) defines the term “act of terrorism” expansively to include any act that is “damaging to critical infrastructure or key resources” and does not differentiate between foreign or domestic terrorism. Basically, under the SAFETY Act, an “act of terrorism” is any act that the Secretary determines meets the requirements under the Act. In its SAFETY Act implementing regulations, DHS defines the term “act of terrorism” broadly to mean “any act determined to have met the following requirements or such other requirements” as defined and specified by the Secretary:

- is unlawful;
- causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a U.S.-flagged carrier or vessel, in or outside the United States; and
- uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.\(^ {843}\)

In the preamble to these regulations, DHS explains its view that the Act does not impose a geographic restriction and that an “act of terrorism”, for purposes of the SAFETY Act, can include an act that occurs outside of the United States provided that it causes harm in the United States.\(^ {844}\) DHS indicated that “harm” in this context includes harm to financial interests.

\(^{839}\) Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response to recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.’

\(^{840}\) 6 U.S.C. § 443 (c).

\(^{841}\) 6 C.F.R. § 25.2.

\(^{842}\) Id. (emphasis added).

\(^{843}\) See 6 C.F.R. §25.2.

\(^{844}\) See 71 Fed. Reg. at 33154. According to DHS, the “focus of the ‘Act of Terrorism’ definition on where harm is realized is appropriate in light of the possibility that an Act of Terrorism may be the result of a series of actions
7.1.4. Criteria for granting SAFETY Act protection

This section discusses the criteria that the Secretary will typically apply in deciding whether to approve an application for SAFETY Act protection.

Congress gave DHS broad discretion in determining whether to approve a product or service but mandated that DHS “shall” consider both technical and economic criteria which must include the following:

- Evidence of prior US Government use or demonstrated substantial utility and effectiveness;
- Availability of the technology for immediate deployment in public and private settings;
- Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of the technology;
- Substantial likelihood that the technology will not be deployed unless SAFETY Act risk management protections are extended;
- Magnitude of risk exposure to the public if the technology is not deployed;
- Evaluation of scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm; and
- Evidence of the technology’s effectiveness in facilitating the defense against acts of terrorism.\(^{845}\)

Under its implementing regulations, DHS has “discretion to give greater weight to some factors over others, and the relative weighting of the various criteria may vary depending upon the particular technology at issue and the threats that the Technology is designed to address.”\(^{846}\) In addition, DHS has regulatory authority to “develop, issue, revise, adopt, and recommend technical standards for various categories or components of anti-terrorism Technologies” and, in considering the criteria, or evaluating whether a particular anti-terrorism Technology complies with any of these standards, the Department “may consider evidence that the Technology is substantially equivalent to other Technologies ... that previously have been” previously approved for SAFETY Act protections.\(^{847}\)

As DHS leadership testified to Congress in 2011, the “majority of criteria stated in the SAFETY Act focus on the effectiveness of those technologies. It is inherently a technical review ... because it is important that those technologies work as expected when they are deployed. If they don’t work, and something happens, someone could die. That is a responsibility that we take very seriously.”\(^{848}\)

In considering the effectiveness of a service or technology and its availability for deployment, DHS will review the steps and supporting activities required by the buyers and users of the product and/or service to deploy, implement, and operate them. DHS will also look at occurring in multiple locations or that the locus of the terrorist act may not be readily discernible. This is especially the case with respect to acts of cyber terrorism.” \(^{71}\) Fed. Reg. at 33154 (emphasis added).\(^{845}\) See 6 U.S.C. § 442(b)(1)-(7).
\(^{846}\) 6 C.F.R. § 25.4(b)(2).
\(^{847}\) Id. at § 25.4(c) and (d).
evidence of consistently positive results; whether reliability and availability are high; whether
the technology or service performs in accordance with specifications; whether the applicant
has proven installation, use and maintenance procedures; whether documented processes
(e.g., training, hiring, technology refresh) are being followed; whether standards are identified
and met; and whether the applicant uses effective Quality Assurance and Quality Control
processes.849

And, in assessing the magnitude of risk exposure to the public if the technology is not
deployed, DHS will likely consider the plausible risks to the public that the technology or
service is designed to counter including fatalities, injuries, economic loss, physical damage,
mass disruption and symbolic damage.850 DHS uses this information to establish, during the
application review process, an appropriate liability cap on the Seller’s damages in the event of
a lawsuit arising from an act of terrorism in which QATT was deployed.

7.1.5. Forms and extent of protection available (Designation and Certification)

The Secretary has authority under the SAFETY Act to provide two distinct sets of protections
for a QATT – “Designation” and/or “Certification.” The protections available under each are
discussed below.

“Designation” by DHS of a product or service provides the following protection:

- exclusive federal court jurisdiction for suits against the Seller of the QATT;851
- a liability cap at the amount of liability insurance specified by DHS;852
- a bar against punitive damages or prejudgment interest;853
- award of “noneconomic damages” (which includes amounts sought for pain and
  suffering, “inconvenience, physical impairment, mental anguish, disfigurement, loss of
  enjoyment of life, loss of consortium, injury to reputation, and any other non-
  pecuniary losses) against the Seller only in direct proportion to the defendant’s
  liability for economic harm (thus precluding the imposition of joint and several
  liability);854
- a bar against noneconomic damages in the absence of physical injury;855 and
- reduction of a plaintiff’s recovery in a suit against the Seller of the QATT by any
  amounts collected by the plaintiff from insurance or other collateral sources.856

Under the SAFETY Act program, DHS may alternatively afford “Developmental, Testing &
Evaluation Designation” (“DT&E”) to certain products or services that it concludes require
additional testing and evaluation.857 The DT&E will include limitations and can be terminated
at the Department’s discretion. Under the implementing regulations, DT&E Designations may
be issued for a reasonable period, but not longer than 36 months.

SAFETY Act “Designation” is a prerequisite for the additional liability protections afforded
to a QATT supplier by a “Certification.” In reviewing an application for SAFETY Act

849 See SAFETY Act Application for Designation and Certification (OMB Control No. 1640-0001, Expires:
03/31/2013), can be found at <www.safetyact.gov> (last visited on 1/23/2013).
850 Id.
851 6 U.S.C. §442(a)(1)
852 6 U.S.C. §443(c)
853 6 U.S.C. §442(b)(1)
854 6 U.S.C. §442(b)(2)(A)
855 Id.
856 6 U.S.C. §442(c)
857 See 6 C.F.R. § 25.4(f).
Certification, the Act requires the Secretary to conduct a more comprehensive review of the
design of such technology and determine whether it will:

- Perform as intended;
- Conform to the Seller’s specifications; and
- Be safe for use as intended.\(^{858}\)

The Act further requires the Seller to “conduct safety and hazard analyses” of its product or
service and supply this information to the Secretary.\(^{859}\)

Thus, the liability protections afforded by a Designation or a Certification are conferred by
two separate actions by the Secretary. Designation of a product or service confers all of the
liability protections indicated above except the rebuttable presumption in favor of the
government contractor defense. In many cases, however, the Designation and Certification
status are conferred by the Secretary simultaneously.

The Seller of a product or service that receives “Certification” is, in addition to the
protections afforded to Designated QATTs, eligible to assert the rebuttable presumption of a
“government contractor defense” in any product liability lawsuit for “claims arising out of,
relating to, or resulting from an act of terrorism, and gains complete liability immunity for
their manufacturers and customers”\(^{860}\)

The government contractor defense, an affirmative defense that immunizes defendants from
certain liability claims, is likely to provide a significant benefit to a the Seller of a QATT in a
lawsuit.\(^{861}\) The defense is derived from the doctrine of sovereign immunity and the principle
that if a contractor works according to government-provided specifications, it is entitled to the
Government’s privilege of immunity and should be protected by that immunity to the same
extent the Government would be if it had performed the work itself. In the leading case of
Boyle v. United Technologies Corp., 487 U.S. 500, 512 (1988), the Supreme Court applied
this doctrine because it concluded that holding contractors liable for damages resulting from
Government contracts would subvert the sovereign immunity protections of the Federal
Government by causing the contractor to pass its costs back to the Government. The Court
explained that it would apply the defense to “shield […] contractors from tort liability for
products manufactured for the Government in accordance with Government specifications, if
the contractor warned the United States about any hazards known to the contractor but not to
the Government.” \(^{Id.}\) However, since then, some federal courts have applied the defense
narrowly and refused to allow its use by non-military contractors. \(^{See, \ e.g., \ In \ re \ Hawaii \ Fed.\}
\text{Asbestos Cases}, 960 F.2d 806 (9th Cir. 1992) (restricting the federal government contractor
defense to military contractors) and \(^{Nielsen \ v. \ George \ Diamond \ Vogel \ Paint \ Co.}, 892 F.2d
1450 (9th Cir. 1990) (restricting the federal government contractor defense to military
contractors providing military equipment). The SAFETY Act expressly extends the
government contractor defense not just to military procurements but more broadly to
companies selling anti-terrorism technology or services to any customer, including private
entities.

Thus, while the government contractor defense “is a judicially-created doctrine”, the express
terms of the SAFETY Act “supplant the requirements of the case law for the application of
the defense” as follows:\(^{862}\)

\(^{858}\) See 6 U.S.C. § 442(d)(2).
\(^{859}\) \(^{Id.}\)
\(^{860}\) 6 U.S.C. § 442(d).
\(^{861}\) \(^{See \ 71 \ Fed. \ Reg. \ at \ 33149.}\)
\(^{862}\) \(^{Id.}\)
- Any Seller of a certified technology cannot be held liable for design defects or failure to warn claims, unless the presumption of the defense is rebutted by evidence that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology. 863
- Once certified, the presumption in favor of the government contractor defense applies in perpetuity to all deployments of the product or service that occur on or after the effective date, as long as it was sold before the Certification’s expiration or termination.
- The presumption in favor of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to the Federal Government or non-Federal Government customers.

Sellers of certified QATTs need not design their products or services to federal government specifications in order to obtain the government contractor defense under the SAFETY Act, nor does the DHS specify any particular technical or technological standards.

If approved for any level of SAFETY Act protection, a non-proprietary description of the approved QATT is listed on the DHS publicly available website (<www.SAFETYACT.gov>) which potential customers can visit to identify technologies with SAFETY Act coverage.

Further, a significant benefit to a successful applicant for either a Designation or Certification is the ability to use a DHS-approved SAFETY Act Mark for its product or service. The applicant must sign a User Agreement prior to receiving the Mark which can then be used in connection with any marketing materials, website advertising or discussions of the technology or service.

DHS has indicated that its evaluation of a product or service “is limited to the requirements of the SAFETY Act and the status of Designation or Certification applies exclusively to the SAFETY Act.” The successful application is “still responsible for complying with all applicable laws, rules, and regulations of any Federal, State, or local agency” with which it would otherwise be required to comply if it had not applied for and received SAFETY Act protections. 864 For instance, if an approved product includes the use of a pesticide that is regulated by the U.S. Environmental Protection Agency under the Federal Insecticide, Fungicide, and Rodenticide Act (“FIFRA”), the granting of SAFETY Act protection does not relieve the holder of the SAFETY Act Designation or Certification of the requirement of complying with FIFRA. In other words, DHS’s independent SAFETY Act evaluation specifically pertains to the efficacy of a particular technology as an anti-terrorism technology but does not address other regulatory requirements.

863 See 6 U.S.C. §442(d)(1): ‘Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.’ Moreover, the Act states that the defense, “shall not in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that - (1) attempts to commit, knowingly participates in, aids and abets, commits any act or terrorism, or any criminal act related to or resulting from such act of terrorism; or (2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.” Id. at § 442(e)(1) and (2).

7.1.6. Insurance requirement and liability limit

As part of a SAFETY Act Designation and/or Certification, the Secretary will set and require the Seller of the QATT to obtain and maintain liability insurance in an amount that the Secretary deems is appropriate “to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism” when the QATT has been “deployed in defense against or response or recovery from such act.” The Act provides that, “in addition to the Seller”, the insurance “shall ... protect ... [c]ontractors, subcontractors, suppliers, vendors, and customers of the Seller” and [c]ontractors, subcontractors, suppliers and vendors of the customer.” The Act then limits the Seller’s liability to the amount of such insurance coverage.

Thus, although the SAFETY Act provides significant limits on a potential third-party liability, it is not a government-provided insurance or indemnification program. As opposed to the liability limitation afforded by the Act, indemnification would involve defending against claims brought against others and satisfying any resulting liability.

The required limits of liability are established by DHS as part of the SAFETY Act application review and will generally depend on both the premium cost and the actual exposures at the time of application. Specifically, the SAFETY Act provides that successful applicants will be required to obtain the “maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price” of the QATT. In accordance with the Secretary’s expressed intent not to set a “one-size-fits-all” numerical requirement for insurance coverage for all technologies that have been designated as QATTs, DHS has indicated that it “may consult with the Seller, the Seller’s insurer and others.” And, in accordance with its implementing regulations, DHS will consider the nature of the technology, the seller’s historic levels of coverage, levels of coverage carried by makers of comparable technology, information regarding the amount of liability insurance offered on the world market, data and history regarding mass casualty losses, and “[a]ny other factor that the [DHS] Under Secretary may consider to be relevant to the determination or to the homeland security of the United States.”

Failure to satisfy any of the insurance requirements, including the requirement to notify the Secretary within 30 days of the issuance of the insurance certification by the Under Secretary, may lead to termination of the seller’s Designation or Certification.

In addition, Designated and Certified sellers of QATTs must enter into reciprocal waivers of claims with their subcontractors, suppliers, vendors and customers (and contractors and subcontractors of the customers) in the manufacture, sale, use, or operation of the QATT, under which each party agrees to be responsible for losses, including business interruption.

866 Id. at § 443(a)(3).
867 Id. at § 443(c).
868 Id. at § 443(a)(2).
869 71 Fed. Reg. at 33,149.
870 6 C.F.R. § 25.4(b). DHS has indicates that it typically sets a minimum amount of liability insurance at $1,000,000 but has not set a maximum cap.
872 See 6 C.F.R. § 25.4(h).
losses that each may sustain, or the losses sustained by its own employees resulting from an act of terrorism when a QATT has been deployed in defense against or recovery from such act. Designated and Certified Sellers must also provide annual certification of insurance coverage to the Under Secretary, and notify the Under Secretary of any change in the type or amount of insurance coverage for the QATT. 873

7.1.7. The application process and timeline

This section discusses the application procedure under the SAFETY Act.

An entity seeking SAFETY Act coverage is required to submit a lengthy and detailed application to the DHS SAFETY Act Office using a DHS-developed Application Kit available on its website. 874 Under the implementing regulations, DHS review is supposed to take no more than 120 days. 875 However, DHS has authority to extend that time period as long it notifies the applicant. 876

DHS provides applicants with opportunities for pre-application consultations and agrees to apply the confidentiality provisions included in the regulations to information obtained during those consultations. 877 This pre-application consultation is available at no cost to the potential applicant. The 120-day regulatory time frame for review has been extended by the Department in order to provide applicants with opportunities to undertake opportunity for pre-application review and to give applicants opportunities to supply additional information requested by the Department. On occasion, DHS has requested applicants to withdraw and resubmit an application in order to address issues identified during preliminary review. 878

Under the SAFETY Act review process, the Assistant Secretary of DHS provides a recommendation to the Under Secretary that the application should be approved or denied, or that additional information is required before a decision can be made. 879 Neither the SAFETY Act nor the regulatory process includes an opportunity for an applicant to comment upon any adverse decision or to appeal it. And the SAFETY Act implementing regulations do not require DHS to state why the application was denied, only that it was denied.

DHS is required, under its regulations, to keep all information submitted by an applicant confidential and exempt from public disclosure. 880 To ensure this protection, the Department screens all application reviewers for conflicts of interests and requires that they sign general nondisclosure agreements as well as conflict of interest statements for each application they review. DHS reviewers typically include personnel from Federally Funded Research and Development Centers, non-profits, the federal government, Federal and National laboratories and academia.

873 6 C.F.R. § 25.5.
874 The web-based, interactive application process allows Sellers to submit applications electronically, obtain automatic feedback on the status of an application, submit questions to a Help Desk to obtain assistance with navigating the application process, and provide access to resource documents and frequently asked questions. The SAFETY Act website contains the electronic application kit.
875 Id.
876 Id.
877 6 C.F.R. § 25.4(e).
878 As noted by Congress, “unlike the patent, trademark, or other license provided by the [US] Government, the Government does not charge a penny to thoroughly review each product for SAFETY Act approval.” See Hearing Before the Subcommittee on Cybersecurity on Infrastructure Protection, and Security Technologies of the Committee on Homeland Security House of Representatives (May 26, 2011) (Statement of Chairman Thompson).
879 6 C.F.R. § 25.5(d).
880 6 C.F.R. § 25.10.
The term of a SAFETY Act approval is typically five to seven years and, to remain effective, must be renewed by DHS each subsequent term.\(^{882}\)

The SAFETY Act’s implementing regulations also provide a streamlined process for providing SAFETY Act coverage for qualified sellers of certain categories of technologies. Under this process, DHS may notify potential sellers that a QATT satisfies the technical criteria for either Certification or Designation and that no additional technical analysis will be required. These streamlined approvals may be issued in response to an application from a seller and/or at the Secretary’s discretion.\(^{883}\) DHS is using this system of Block Designations and Certifications as “powerful tools to incentivize deployment of anti-terrorism technologies and offer an expedited review timeline.”\(^{884}\) Recognizing that “the SAFETY Act application process requires a significant investment by the applicant” and that Block Designations “are processed 25 percent faster than standard applications,” DHS has found this initiative has strong industry interest.\(^{885}\) An example of an approved Block Designation and Block Certification is for standards development organizations who wish to seek SAFETY Act coverage for national standards that have been formally adopted by DHS as DHS National Standards. DHS leadership has explained that “[t]he intent of this initiative is to provide incentives for increased use and more widespread implementation of anti-terrorism standards, by significantly expanding the pool of standards eligible for SAFETY Act coverage.”\(^{886}\)

### 7.1.8. Assessment of effectiveness, and advantages and disadvantages

Assessment of the effectiveness of the SAFETY Act is necessarily something of an exercise in extrapolation. Information on the implementation of the Act in practise is not publicly available, nor has a review of its operation and implementation been undertaken as yet. Moreover, there is necessary to point again to the unique litigation and legal landscape that characterises the context in which the SAFETY Act operates. This section will draw on several indicators in attempting to evaluate the relative effectiveness of the SAFETY Act, and the advantages and disadvantages associated with it under such metrics.

There are several prisms through which the relative effectiveness of the act may be approached. First, one can consider the number of applications that the Department has reviewed and approved. Despite what some in Congress considered a slow start, in Fiscal Year 2011, DHS approved 101 applications, more than 40 percent above Fiscal Year 2010 and 20 percent above the previous record, reached in Fiscal Year 2007.\(^{887}\) Since the inception of the program, DHS has approved more than 400 applications and stated that “these technologies have been widely deployed to protect commercial facilities, critical infrastructure, transportation hubs, ports, borders, sports venues and commercial aviation.”\(^{888}\) DHS has concluded that these approvals, combined with the breadth and variety of products

---

\(^{882}\) DHS has also awarded SAFETY Act protections to apply retroactively to past deployments of the QATT.

\(^{883}\) See 6 C.F.R. §§ 25.6(h), 25.9(j).


\(^{885}\) See, id., (“Our goal is to streamline our Block review process and speed processing timelines to be 30 to 50 percent faster than standard applications and provide an expedited review path for appropriate technologies”).

\(^{886}\) Id.

\(^{887}\) S&T Directorate, FY2011 Year in Review at 47.

\(^{888}\) See Benda Testimony.
and services approved, indicate that the targeted industry appears to be engaged and motivated to use the program.

A second factor is to consider in gauging the effectiveness of the program is how SAFETY Act Designations and Certifications have impacted the marketplace. Specifically, increased sales, deployment of technologies, and evidence of rising research and development budgets can indicate success. Private companies have testified as to the positive impact of SAFETY Act benefits for them. And, increasingly, SAFETY Act awards are being aligned with federal contract awards where the same anti-terrorism technology is involved. Most notably, in 2007, the Federal Acquisition Regulations were amended to mandate that federal government agencies consider whether their homeland security procurements are eligible for SAFETY Act coverage.

An additional factor in measuring the SAFETY Act’s effectiveness is the scope of products and services which have been approved by the Department. Since the inception of the program, the Secretary has reviewed and approved a broad spectrum of anti-terrorism products and services including security screening equipment (including security guard training and management, portal detectors, perimeter detection technologies, and security service providers) and methodologies and providers of vulnerability assessments. This broad range of technologies included products, services, software, and other forms of intellectual property. In some cases, these products and services have not been newly developed but have been employed previously. Some specific examples of successful applications include coverage to a chemical company that implements comprehensive security plans internally to protect its own facilities, to the Port Authority of New York and New Jersey for certain of their security-related activities, and to the Cincinnati/Northern Kentucky International Airport for its “Airport Security Management Plan.” DHS has also approved a technology that provides cybersecurity situational awareness and network security monitoring, a technology undergoing testing and evaluation designed to provide cybersecurity protection for the smart grid, an integrated system technology undergoing testing and evaluation designed to provide situational awareness for the Port of Long Beach, California, a modular, rapidly deployable floating security barrier system designed to protect targets from high speed small boats, a process for the production of an ammonium nitrate fertilizer treated to render it less detonable than standard fertilizer, onsite production system for chlorine at water treatment plants (eliminating transport risk of bulk chlorine), threatening object- and explosive-detection systems deployed in the nation's airports, a web-based software tool that integrates a first responder decision support system with geospatial information technology, an acoustic detection system to detect and rapidly triangulate gunshots and explosive event sounds, and explosive containment vessels, allowing for the safe containment, transport and disposal of explosive devices (used in response to the Times Square bombing attempt in May 2010).

---

889 In 2012, Secretary Janet Napolitano reported that small business applicants accounted for more than 50 percent of SAFETY Act applications and awards (150 percent of goal) and that the average processing time for applications was maintained below the 120 calendar day timeframe mandated by Congress.

890 See, e.g., Statement of Scott Boylan, Vice President and General Counsel, Morpho Detection, Inc. before Congressional Committee on Homeland Security (May 26, 2011) (“The transfer of SAFETY Act coverage . . . was a pre-condition to closing when our company was sold by GE to Safran in 2009. This only serves to illustrate how important this coverage is to investment decisions.”); Statement of Craig A. Harvey, Chief Operations Officer and Executive Vice President, NVision Solutions, Inc. (“By levelling the playing field and capping financial exposure The SAFETY Act encourages innovation. Without the SAFETY act, our desire to bring [our anti-terrorism technology] to market may never have been realized.”

891 See 40 C.F.R. Parts 50 and 52.


The use of the DHS-approved SAFETY Act Mark, discussed above, is widely seen in the marketplace as another good indication of the program’s effectiveness. Use of the SAFETY Act mark provides some assurance that the products or services have bearing the mark been properly vetted by the federal government and meet stringent criteria for effectiveness and usefulness, making its use valuable for successful applicants.\textsuperscript{894}

DHS has not released any formal cost/benefit assessment of the US SAFETY Act or data quantifying the advantages and disadvantages of the program have not been quantified. As the above analysis of the efficacy suggests, however, qualitatively, the SAFETY Act program appears to have provided significant advantages to both government and the private sector including the following:

- increased incentives for innovation and deployment of technology;
- the resulting greater and faster availability of anti-terrorism technology, product and services; and
- the greater security resulting from their availability.

Indeed, industry indications signal that the Safety Act has encouraged US SI providers to develop security technologies. To the extent that these technologies are also attractive in the EU market, the Act has helped those companies that developed them to be able to compete in the EU market as well. In the same way, to the extent EU liability limitations encourage the development of security technologies by EU companies, those companies can then compete in the US market with those technologies, and be eligible for protection under the US Safety Act as well.\textsuperscript{895}

The advantages presented above are believed by many in US government and in the private sector to be significant. For example, the US Congress has recognized that in light of tighter federal budgets, the federal government must rely increasingly on the private sector which it believes “has enormous research and development capability” and can, therefore, provide “DHS with a necessary tool to access large private sector investments in the homeland security marketplace for the protection of all Americans.”\textsuperscript{896} Because these benefits have not been quantified, however, no reliable indication can be given of how strong these incentives have been, or how many technologies and products would not have been introduced but for the SAFETY Act.

Potential disadvantages of the SAFETY Act program are somewhat speculative, because no claims have been made against participating companies and no other disadvantages have come to light. In theory, potential disadvantages could include the following:

- Premature release and deployment of technology that has not been sufficiently tested. This is unlikely, however, because the government reviews the technology concerned prior to extending SAFETY Act benefits; and
- Unavailability of compensation to plaintiffs that have been harmed by the products and services deployed by defendants that benefit from protection under the SAFETY Act. No such cases have arisen, however, and the liability protection offered by the SAFETY Act is conditional and not complete; the insurance requirement ensures that compensation is available in appropriate cases.

\textsuperscript{894} In fact, some companies have internal acquisition policies to prioritize purchase of technologies and services that bear the SAFETY Act mark of approval.
\textsuperscript{895} Stakeholder response to Questionnaire in Annex II.
\textsuperscript{896} Lungren Statement.
Protection of culpable parties through the exclusive remedy provision where, in the interests of justice, other actors in the supply chain would otherwise be named respondents but plaintiffs are debarred from pursuing them as claims must be directed at the QATT producer;

Concern also subsists about how strong the protections of the SAFETY Act are if an act of terrorism occurs overseas while the anti-terrorism product or service is deployed. DHS has also stated in its regulations that if an attack overseas results in harm within the United States, the SAFETY Act will apply, but some are concerned that more should be done to solidify protections similar to the SAFETY Act in foreign nations or to encourage foreign nations to formally recognize the applicability of the SAFETY Act for acts of terrorism occurring on their territory. In other words, the SAFETY Act effectively manages excessive liability exposure by requiring successful applicants to maintain adequate liability insurance and offering limiting liability protections in return.

7.2. US case law pertaining to third party liability compensation against security industry

Congressional motivation to enact the SAFETY Act stemmed primarily from its reaction to the significant liability risks that, Congress concluded, were inhibiting the private sector from developing and selling anti-terrorism technologies. These risks were heightened by the litigation and court rulings that followed the 9/11 attacks and litigation related to the 1993 World Trade Center bombing. These lawsuits, among other things, exposed private industry and government entities to extraordinary costs based upon potential findings that their services and products were inadequate to address the risks of terrorist attack and, thus, responsible for the damages suffered by victims and their families.

Immediately after 9/11, lawsuits were filed by victims and their families against a wide swath of defendants, including the aviation industry and their security companies. In response to the perceived threat that the aviation industry would collapse under the weight of crushing jury verdicts, Congress passed legislation which capped the airlines’ liability, provided subsidies to protect the airline industry, and established the Victims Compensation Fund (“the Fund”) giving injured and families of the those killed in the attacks the option of making a claim and, thereby, forfeiting their right to sue the airlines or other possibly responsible parties in personal-injury or wrongful death suits. Claimants under the Fund would not have to prove fault or show a duty to pay on the part of the defendant, and payment through the Fund would be made within a relatively short period. The amount of the claimant’s compensation, however, may be less than possible recovery from lawsuits, and punitive damages would not be available.

Some of the injured and families of the deceased as well as several property damage claimants opted out of the Fund and filed suit in the United States District Court for the Southern District of New York against the air carriers (United and American Airlines) and the airport security companies affiliated with those air carriers (called collectively “Aviation Defendants”). Also included as defendants were the Port Authority of New York and New Jersey and the Boeing Company (the manufacturer of two of the airplanes involved in the attacks). The plaintiffs alleged, in pertinent part, that the defendants were responsible in some part for the loss of life and property.

---

The plaintiffs argued specifically that the Aviation Defendants were directly responsible for their harms because they allegedly allowed the terrorists to hijack commercial airplanes and crash. The Aviation Defendants moved for dismissal on the grounds that they did not owe a duty to protect plaintiffs on the ground from terrorists and, in the alternative, if they did owe a duty, the 9/11 attacks were so extraordinary and unforeseeable as to be intervening and superseding causes sufficient to break the causal link between the defendants and any potential liability.  

The Aviation Defendants conceded that they “owed a duty to the crew and the passengers on the plane” but that “they did not owe any duty to ‘ground victims’.”

The Aviation defendants also moved to dismiss the claims against them on the grounds that the terrorist attacks represented an unforeseeable criminal act that should sever any liability. This defense had been used successfully in lawsuits stemming from the earlier 1995 Oklahoma City bombing. Defendants in 9/11 lawsuits anticipated that these same defenses would apply, but the federal court ruled that the claims of the plaintiffs could move forward because the defendants were deemed “warned” of the threat of terrorism, especially against targets in New York City, and if a defendant knew or should have been aware of a terrorist threat, it had a duty to take reasonable measures to mitigate the threat or face liability in the event of an attack.

Judge Hellerstein rejected these claims holding that even private companies owe a duty of care to people who work in the nation’s critical infrastructure and count on others to protect them. Judge Hellerstein concluded that “plaintiffs and society generally could have reasonably expected that the screening performed at airports by the Aviation Defendants would be for the protection of people on the ground as well as for those in airplanes” and that “[t]he airlines, and the airport security companies, could best screen those boarding, and bringing objects onto, airplanes.” Judge Hellerstein went on to conclude because the Aviation Defendants “controlled who came onto the planes and what was carried aboard, they had an obligation to take reasonable care in screening precisely because of the risk of terrorist hijackings, and the dangerous consequences that would inevitably follow.”

Responding to the 9/11 suits against it alleging faulty cockpit doors, Boeing (the airplane manufacturer), argued in part that they could not have foreseen the terrorist attack and so there should be no liability on its part. Rejecting this argument, Judge Hellerstein declined to rule, as a matter of law, that Boeing could not foresee forced entry into the cockpit by terrorists and held that Boeing had a duty to prevent unauthorized access to the cockpit, which could present risks to persons on the ground.

In 2011, the United States Court of Appeals for the Second Circuit approved a settlement resolving the bulk of the 9/11-related property damage and insurance subrogation claims against airlines and their security companies (including both providers of security services and suppliers/ producers of security goods and equipment) for an aggregate settlement amount of $1.2 billion. A group of plaintiffs that elected not to participate in the mediation of the case

---

900 Under US law, a motion to dismiss under Rule 12(b)(6) is basically a test of the plaintiff’s ability to craft a sustainable pleading; it is not a test of the strength of the underlying claims.
901 Id. at 288-289.
903 See In re September 11 Litigation, 280 F. Supp. 2d at 279.
904 Id. at 287.
905 Id. at 292-293.
906 Id. at 296.
had challenged the proposed settlement. In affirming the proposed settlement, the Second Circuit rejected arguments that the Air Transportation Safety and System Stabilization Act of 2001 ("ATTSSA") preempted New York law, that the settlement was not fair, and that the defendants’ settlement payments could not be credited towards their liability limits under the ATTSSA. 907

Similar to Judge Hellerstein’s rationale in the 9/11 litigation, in 2008, a New York appellate court upheld a jury’s finding of liability against the Port Authority of New York and New Jersey, the landlord of the World Trade Center, resulting from the 1993 terrorist attack against the building. 908 Notably, the jury apportioned the liability finding the Port Authority to be 68% liable in the attack for its negligence in failing to provide security in the face of a clear danger that the trade center was a terrorist target and found the terrorists only 32% liable for the attack. The New York appellate court stated that “the evidence overwhelmingly supported the view that the conscientious performance of defendant’s duty reasonably to secure its premises would have prevented the harm. This civil jury had no power to decide whether the terrorists should in any meaningful sense be ‘absolved’ of their murderous acts. What it could and did decide was rather that the acts of these terrorists, even while obviously odious in the extreme, were not a cause for the easy absolution of this defendant from its civil obligations.” 909

Even before the events of 9/11, various civil litigation following terrorist attacks imposed liability on industry. In the civil litigation following the Pan American flight bombing, the airline was found negligent by providing an opportunity for terrorists to plant the bomb on their equipment. 910 And, after the first bombing of the World Trade Center, a State court held the Port Authority of New York/New Jersey liable for failure to implement prior vulnerability assessment recommendations. 911

7.3. Assessment of the potential of the US SAFETY Act to shield European security industry against limitless third party liability

The extent to which the US Safety Act can shield EU-based companies against limitless liability is chiefly a function of two parameters:

- The geographic scope of application of the Safety Act; and
- Whether EU-based companies and technologies developed in the EU are eligible to benefit from the protection offered by the Safety Act on the same footing with US companies.

Each of these two factors are discussed in turn below.

907 See In re September 11 Property Damage Litigation, No. 10-2970 (2d Cir. April 8, 2011).
909 Id. at 359
911 See In re World Trade Ctr. Bombing Litig., 709 N.E.2d 452, 455 (N.Y. 1999) (stating the result of the Appellate division, which was reversed in this decision). However, the court did not hold the fertilizer manufacturer of the material used to detonate the homemade bomb liable, because it found the manufacturer did not have a duty to the public to prevent terrorists from using ammonium nitrate fertilizer. Port Auth. v. Arcadian Corp., 189 F.3d 305, 317 (3d Cir. 1999). See Port Auth. v Arcadian Corp., 189 F.3d 305, 317 (3d Cir. 1999).
7.3.1. Geographic scope of application

As a general principle, the Act applies only within US territory, i.e. to liability claims filed before US courts. The Act is limited to harm that occurs in US territory but applies also terrorist activities that may have occurred entirely outside of US territory. Therefore, under the Act, a connection must be established between an attack on foreign soil and harm, including financial harm, within the United States. This connection can influence whether an action is ultimately deemed an “act of terrorism” for purposes of SAFETY Act coverage. Even if the activity is deemed to be a terrorist act, however, in the event an act of terrorism physically occurs outside the United States, there is the distinct probability that a suit could be brought in the foreign jurisdiction where the SAFETY Act would not apply.

Questions have been raised about a proposed amendment to the US Safety Act that was discussed in 2011 within the US Aerospace Industries Association (AIA) Homeland Security Limited Liability Working Group. This amendment would confirm coverage in the United States for both US and EU homeland security manufacturers from events happening overseas, regardless of the specific circumstances of the incident. The amendment, of course, would have no effect in EU courts, just as the Safety Act has none there today. Regardless, this amendment is not pending and we are not aware of any plan to propose it.912

The situation is different if claims are brought before the courts of other countries. Whether a non-US court may give effect to the protection granted pursuant to the US SAFETY Act in relation to companies and technologies that benefit from its protection, is a question of the national law that the court must apply, including the conflict of laws rules and the applicable law. It is conceivable that if a non-US court concludes that US law applies, it would recognize the protection granted pursuant to the Act. This, however, is a national law issue that is not governed by the SAFETY Act or any other US law.

7.3.2. Eligibility of EU-based companies

As discussed in section [], above, the SAFETY Act authorizes liability protections to be extended to “Sellers” of so-called “Qualified Anti-terrorism Technologies” (QATTs). The definition of Seller, which covers “any person, firm, or other entity that sells or otherwise provides” a QATT, does not exclude EU-based companies. The term QATT is also defined in a way that can encompass technology designed, developed, or modified in the EU, if it is intended for the purpose of “preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause.”

Thus, EU-based companies that intended to place qualifying technology on the US market are eligible for protection under the SAFETY Act. Like US companies, EU companies, of course, must submit an application to DHS and the requisite information and materials, and follow the procedure under the SAFETY Act. As a practical matter, it may be more expensive for non-US companies to obtain designation or certification under the Safety Act, since they may incur higher information, administrative, and transaction cost, including fees for advisors.

Otherwise, EU SI providers have been able to secure the same benefit from the US Safety Act that US SI providers enjoy. The Safety Act does not differentiate companies on the basis of nationality. The US wants to invite the best products to market to secure its people and property regardless of the country of origin. Indeed, all companies - irrespective of their country of origin - can submit applications for Safety Act approval and protection. Over 600

912 Stakeholder response to Questionnaire in Annex II.
anti-terrorism technologies, including a wide range of products, services, and industry standards, have been granted protection under the Act. Examples include hardware/software products (physical barriers, screening/detection equipment and consoles, unmanned aerial platforms), services (canine screening teams, cargo screening, engineering & integration, security consulting), and standards (fire protection/electrical codes, public water utilities, architecture & design). European companies such as Smiths Detection, BAE Systems, Securitas, Safran, Siemens, and BIVAC N.A. have availed themselves of such protection under the Safety Act:

- Smiths Detection: 10 Safety Act coverages, including x-ray detection equipment and related maintenance, explosive detection scanners, web-based surveillance sensor management software, bio-agent detection, crisis management systems.
- BAE Systems: 5 coverages, including Energy Absorbing Walls, Cable & Piping Shields, communications systems, infrared imaging and countermeasures systems.
- Securitas: 4 coverages, including security assessments and consulting services, protective and response services.
- Safran: 4 coverages, including explosive detection/screening equipment and related logistics and maintenance support and services.
- Siemens: 3 coverages, including Checked Baggage Inspection systems, Systems Engineering and Integration Services for nuclear detection systems, maintenance and repair services for security screening equipment.
- BIVAC N.A.: 1 coverage, for Third Party Validation Services offered in support of the Customs-Trade Partnership against Terrorism (C-TPAT). 913

7.4. Analysis of the differences between the US federal legal system and the necessary European Union supranational framework preconditions to conclude a similar legal act

The Safety Act, of course, is specific to the US with its complicated and rich civil liability system. The US tort liability system includes Federal and State law, and substantive law and civil procedure. The liability exposure of security companies is a function of this system, and this exposure necessitated the Safety Act.

The European liability landscape and litigation environment is different in many respects. These differences may affect the necessity of a Safety Act-like regime, as well as the way in such a regime could be designed. In this section, the focus is on the latter aspect. For each feature of the Safety Act, we identify the closest corresponding possible features of the EU legal tradition which would allow replication of the SAFETY Act regime in the EU.

The Safety Act regime includes features that can be regarded as (1) institutional, (2) procedural, and (3) substantive. The following are the key features of the Safety Act in each of these three categories:

(1) Institutional:
- The protection of the Safety Act is granted upon application by a Federal agency (the Secretary of Homeland Security); and
- The Act creates an exclusive federal cause of action against sellers of anti-terrorism technologies for claims arising out of an act of terrorism, which means that state courts no longer have jurisdiction to hear such claims.

913 Stakeholder response to Questionnaire in Annex II.
(2) Procedural:
- The Safety Act requires that a procedure be established to review and make decisions on applications for protection;
- A procedure is necessary too for the publication of the decisions made pursuant to the Safety Act; and
- A procedure for the supervision of the use the Safety Act mark is required.

(3) Substantive:
- The Safety Act limits liability exposure by (i) excluding punitive damages and prejudgment interest, and (ii) excluding recovery for non-economic damages in the absence of physical injury, (iii) limiting recovery for non-economic damages in proportion to the defendant’s liability for economic harm, and (iv) reducing recovery in a suit against the seller of the QATT by any amounts collected by the plaintiff from insurance or other collateral sources;
- The Safety Act authorizes the Secretary to set a liability cap at the amount of liability insurance specified by DHS based on the maximum amount of liability insurance reasonably available from private sources;
- Further, the Safety Act creates a rebuttable presumption of a “government contractor defense” in any product liability lawsuit.

For each of these features, we discuss analogous features within the European legal landscape which could allow for the introduction of similar features as well as the particular aspects of the EU legal framework and landscape which would hinder or disallow such efforts. Before doing so, however, a brief analysis of some preliminary issues relating to EU’s scope of authority and the current structure of the civil liability landscape in Europe is presented.

7.4.1. EU powers and legislation regarding TPL of the security industry

Under Article 4(2) TEU, national security remains the sole responsibility of each Member State. Thus, the EU does not have the power to legislate directly on national security. Further, Article 346 TFEU (ex Article 296 TEC), under (b), provides that ‘any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes.’ Pursuant to Article 73 TFEU, ‘it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.’ Although not directly relevant to the issue of allocation of powers, Article 6 of the Charter provides that ‘everyone has the right to liberty and security of person.’

Thus, national security policy is not a power of the EU. It should be noted, however, that legislation on third party liability (TPL) of the security industry is not national security policy. Like other policies and laws, such legislation may indirectly influence national security policy, but is not part thereof. This raises the question what the legal basis could be for EU legislation on TPL of security providers. The EU does not have explicit powers to legislate on civil liability, but liability legislation may be covered by another EU competence.

The issue of the security industry’s third party liability plays out differently in different Member States. The nature and magnitude of the liability exposure varies based on the national law of the Member States. Differences in liability exposure could result in different competitive conditions and in barriers to trade between the Member States. For instance, a security provider from a Member State where the liability exposure is low, may be reluctant
to sell products in a Member State where the liability exposure is high. This may be so, for instance, where a security provider does not have adequate insurance in place, because such insurance is not needed in his home country. Thus, differences in third party liability exposure of security providers may, indirectly, result in differences in security levels between Member States, and differences in security levels, in turn, may affect movement of goods, persons, and capital between the Member States.

Because differences in TPL between the Member States may affect the free movement and frustrate the objective of establishing an internal market, the EU may be able to exercise its powers pursuant to the internal market title of the TFEU. Article 26 (ex Article 14 TEC) provides that the EU ‘shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties.’ To this end, the ‘internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.’

In legislating, of course, the EU, of course, must respect the relevant provisions of the Treaty. For example, EU legislation should meet the subsidiarity and proportionality principles set forth in the TFEU. As Article 5 puts it, ‘[t]he use of Union competences is governed by the principles of subsidiarity and proportionality.’ Any EU TPL legislation, of course, would have to comply with these principles.

Thus, the conclusion is that there is no express prohibition for the EU, based on its internal market powers, to adopt TPL legislation for the security industry, including legislation along the lines of the US Safety Act, subject to compliance with the Treaty. Such legislation, of course, also raises a series of more specific issues, the more significant ones of which are discussed in the next section.

7.4.2. Institutional, procedural and substantive issues

As discussed above, the main features of the US Safety Act should be reviewed to determine whether they apply to the EU’s situation, and if so, what role they could play in the EU context.

7.4.2.1. Institutional

As far as the institutional context is concerned, two significant features are discussed in turn, below.

- The protection of the Safety Act is granted upon application by a Federal agency (the Secretary of Homeland Security).

  The entire process of preapplication review, consultation, and application processing and approval is administered at a centralized level through a Federal agency, staffed by Federal experts and in receipt of Federal funding, as well with access to the outputs and personnel of other related Federal research projects or centers.

No such agency already exists within the EU. This would mean that either an existing or newly established EU agency or the Commission would grant TPL protection and that expertise in security matters would need to be quickly collated and accumulated by/for such entities. As far as existing agencies are concerned there is no immediately analogous entity that could assume the role readily, although given the nature of the analysis that is necessary
in connection with the review of applications, an argument could be made that the European Patent Office could potentially be involved in the process.

It is, of course, also conceivable that an entirely new agency is established for this purpose. If the discretion involved in granting TPL protection is significant, however, it may be more appropriate for the Commission to make these decisions. Certainly, it is not the case that a specifically-created EU agency, or network of national Member State-based agencies could exercise the same degree of discretion afforded to the Under Secretary and Secretary of the DHS. To recap, the Secretary’s discretion is reserved in defining an ‘act of terrorism’, on how the specified criteria are to be applied during the application process, on the weighting to give to any particular criterion over another during the application process, and on the award of Developmental, Testing and Evaluation Designation to applicants. Such delegation of discretionary powers is not valid in the European Union as it usurps the proper position of the EU institutions and the Courts. The long-established Meroni rule stipulated that the delegation of such executive powers to an agency must involve powers which are clearly defined, and to exercised “subject to strict review in light of objective criteria determined by the delegating authority”.914 This means that the powers that are currently vested in the Secretary of the DHS could arguably not be vested in an agency, or network of agencies as they are, but would have to be re-defined along objective criteria that would minimize the level of discretion afforded in their exercise. This in itself creates renewed problems in terms of determining the delineation and scope of nebulous ideas such as ‘act of terrorism’ and defining qualifying-product standards. In the absence of existing agency and experience with this area this is likely to involve considerable expense, as well as running the risk that, if improperly defined, the operation of such definitions could operate to the detriment of the schemes entire purpose, for example, by allowing liability in certain cases where actions are deemed to fall outside the scope of an ‘act of terrorism’.

The third institutional option is to utilise or create national agencies of the Member States to administer and make decisions on applications. This could be combined with a rule requiring that ruling by a Member State have validity throughout the EU, through some form of mutual recognition or otherwise.

- The Act creates an exclusive federal cause of action against sellers of anti-terrorism technologies for claims arising out of an act of terrorism, which means that state courts no longer have jurisdiction to hear such claims.

One of the problems here is that there are no ‘federal’ courts in the EU, other than the European Courts, which have limited jurisdiction and are currently not competent to hear any civil liability cases involving private parties as defendants. In theory, it would be possible to expand the jurisdiction of the EU courts so that it could hear claims by private parties in relation to third party liability covered by the regime of the EU ‘Safety Act’-like legislation. This would be an unprecedented extension of the Court’s jurisdiction, and would require substantial political will and a change to the European Treaties.

The second problem is that the national courts would have to be deprived of jurisdiction they otherwise have, because the EU courts would have exclusive jurisdiction. There is no relevant precedent in this respect, although as noted

7.4.2.2. Procedural

- **The Safety Act requires that a procedure be established to review and make decisions on applications for protection.**

Review of applications in and of itself should not present any major obstacle; there are many procedures involving review of applications currently carried out under Union-level auspices. However, replicating the SAFETY Act review process does present some particular problems, foremost among which is the nature of the stringent review procedure that is engaged in. Once a thorough internal review has been conducted under the SAFETY Act, applications are further subjected to a peer-review evaluation process, analyzing each application against the criteria specified under the Act. This peer-review process relies on the availability of experts from within the Agency, as well as from other federally-funded research and development centers and agencies. Indeed since its inception the ‘Office of SAFETY Act Implementation’ the DHS’s dedicated expert application review body has grown steadily. In the EU context, however, because an agency or network of such agencies would have to be created, or at least coordinated, replication of this aspect of the process is likely to prove onerous and potentially prohibitively expensive.

- A procedure is necessary too for the publication of the decisions made pursuant to the Safety Act.

In practice, this should be straightforward. Decisions could be published in the EU Official Journal, in national official journals, or a publicly accessible database (such as the ECHA’s database of registration of chemical substances), with a copy notified to the Commission. A central register would be useful.

- A procedure for the supervision of the use the Safety Act mark is required.

If the EU Safety Act were to include a mark, the supervision of the use of such a mark could be performed by the Commission, the competent EU agency, and/or the Member States.

7.4.2.3. Substantive

- **The Safety Act limits liability exposure by (i) excluding punitive damages and prejudgment interest, and (ii) excluding recovery for non-economic damages in the absence of physical injury, (iii) limiting recovery for non-economic damages in proportion to the defendant’s liability for economic harm, and (iv) reducing recovery in a suit against the seller of the QATT by any amounts collected by the plaintiff from insurance or other collateral sources.**

There is no precedent for such rules in EU law. Having said that, there would not appear to be a strong need for such rules, given that Member State civil liability regimes do not provide for punitive damages. In the EU, compensation for pain and suffering and moral damages tend to be low compared to the US, and the collateral sources of compensation including insurance generally reduce the amount of compensation available in civil law suits.

- The Safety Act authorizes the Secretary to set a liability cap at the amount of liability insurance specified by DHS based on the maximum amount of liability insurance reasonably available from private sources.

This would be unusual, but such a rule would technically be possible as a matter of EU law. Under national law, the amount of compensation awarded may be mitigated based on factors such as the insurance coverage limit of the defendant. Again, however, this would have to be
determined according to pre-determined rules which would be difficult to define, and would have to be applied in a standardized fashion if a network of Member State agencies were engaged or the system would be vulnerable to claims under competition law.

- Further, the Safety Act creates a rebuttable presumption of a “government contractor defense” in any product liability lawsuit.

This defense is not generally available under the national laws of the Member States, nor indeed is the idea of sovereign and sovereign-derived contractor liability.

The conclusion is that the key features of the US Safety Act could be implemented under some EU level TPL limitation regime. Many specific issues, however, would have to be analyzed and resolved and would involve extensive incursion into unprecedented areas of EU law and tradition.
Chapter 8 Conclusions and policy options

This chapter discusses policy options derived from the previous work packages. The options and possible scenarios for both European policy makers and also for other concerned actors, like the security industry, are described in a comprehensive and easily comprehensible and comparable way. Legal as well as practical implications are presented in detail and weighed against each other. Legal "worst case scenarios" have been developed in relation to each option.

The following tasks are part of this Work Package. Task 6.1 involves feasibility options and scenarios including (i) liability capping schemes, (ii) liability exclusion schemes, (iii) litigation management, excluding the possibility of multiple litigations against a seller of qualified security technology or services, (iv) various forms of liability compensation funds (e.g. victim compensation fund), (v) recommendation on third party liability limitation by the European Commission, (vi) EU Member State in which an incident would occur would also be the place of exclusive jurisdiction, (vii) other exclusive jurisdiction options, and (viii) other legal options leading to precautionary third party liability limitation. Task 6.2 requires a description and rating of comparative disadvantages that could arise for the European security industry due to the lack of an EU-wide third party liability regime. Finally, Task 6.3 focuses on the pros and cons of various third party liability options including the necessary prerequisites in institutional European law as well as representative "worst case scenarios."

The analysis presented in this chapter covers all three tasks of this Work Package. To allow for easy comparison and avoid repetition, we present the results of our analysis in an integrated fashion, rather than following exactly the structure of the work packages.

A few starting points will be taken as foundations for the normative analysis provided in this chapter. We will e.g. take into account generally recognized goals of a liability regime, including reparation and deterrence. From a law and economics perspective, we will adopt the approach proposed by Guido Calabresi\(^{916}\) who argued that the goal of a liability system should be to minimize the total sum of primary, secondary and tertiary accident costs. The primary accident costs in that respect refer to the cost of accident avoidance and the expected accident costs; the secondary accident costs refer to the cost of loss spreading and the tertiary accident costs refer to the administrative costs for the functioning of the liability system. Hence, starting point will be that a liability regime has particular goals in providing prevention/deterrence of accidents and hence has an important role to play in society in terms of maximization of social welfare. In addition, the loss spreading goal (reduction of secondary accident costs), meaning distribution of losses and victim compensation, will be taken as starting points as well.

An important starting point also derives from the lessons from the comparative analysis based on EU Member States legislation and related case law. That legal analysis\(^{917}\) clearly showed that Member States do not treat the security industry differently than any other industry. Although liability of the security industry is predominantly fault based, it is not impossible that the security provider can be held liable if damage is caused by a natural disaster or by an intentional act by a third person. There are hence important functions of a liability of the security industry, both from the economic perspective (providing prevention/deterrence and

---

\(^{915}\) This corresponds to Work Package 6 of the Invitation to Tender.

\(^{916}\) Calabresi 1970.

\(^{917}\) Provided in chapter 4 above.
loss spreading) as well as from a comparative perspective (starting from the status quo of the legal regime in the Member States today).

The first part of this chapter addresses the critical question whether the EU security industry needs separate treatment for liability purposes (task 6.2). We explore the question whether there is there a serious liability threat for security industry in Europe today or whether such a threat is likely, and how the security industry may be different from other sectors of industry that could potentially be exposed to liability for large scale damage. This analysis will build on the outcomes of the previous work packages. It will also involve an analysis of the differences between the US and EU in terms of liability exposure, which may help to explain why the US adopted the Safety Act and the EU has not yet done so. We will analyse and discuss arguments presented by the security industry from a policy and economic perspective, including the close link with the government, and with national security, which raises a question whether its situation is comparable to state immunity. The potential disadvantages of liability limits are examined in terms of the goals of liability, including incentives and distributional issues (8.1).

In section 8.2, options for limiting liability and their respective pros and cons are discussed. The options that will be analysed are derived from the previous work packages and include (i) limitation of compensation to particular heads of damages (liability exclusion schemes, e.g., of pure economic loss), (ii) liability capping schemes, based on Work Package 4.1, (iii) channelling of liability to other private parties or the government (with examples from Work Packages 3.1, 3.2 and 3.2), (iv) limiting causation (e.g. by designating certain damage as too remote), (v) linking liability to regulation, so that compliance with regulation excludes liability (regulatory compliance preclusion or defence), and (vi) mandatory financial security (e.g. as in the case of many of the international law treaties on civil aviation, nuclear safety and environmental liability discussed supra in chapter 5). For each option, the pros and cons will be analysed, also in light of ‘worst case’ scenarios.

The third section of this chapter explores procedural solutions that do not involve a change in the substantive liability rules, but only in the procedure for resolving claims. We will discuss (i) litigation management, notably, excluding the possibility of multiple cases in multiple Member States, (ii) designating the EU Member State in which incident occurs as the place of exclusive jurisdiction, and (iii) other exclusive jurisdiction options, relying on the results of Work Package 1.5 (8.3).

Section 8.4 briefly discusses human rights aspects of liability and limitations on liability. Section 8.5 addresses victim compensation solutions, including (i) a possible victim compensation fund, (ii) government provided compensation, and (iii) mandatory first party insurance, relying on the outcomes of Work Package 4.4.

In section 8.6, we set out a presentation of the prerequisites in institutional European law (task 6.3), and explore whether the EU possesses the powers to legislate in this area and, if so, under which general conditions (8.6). Finally the options and their pros and cons will be evaluated (8.7).

8.1. Separate treatment of the security industry?

Starting point for this project was that there is a serious actual liability threat for the security industry in Europe or at least a likely threat in the future which would justify a separate treatment of the security industry. To put it bluntly the question therefore arises whether the security industry would be in a different position than the position of any other industry (like e.g. the petrochemical industry, the upstream and downstream energy industry etc.) that could also be exposed to substantial liability risks. The question therefore is whether the security
industry is that substantially different that, from a policy perspective, it merits a different treatment, i.e. its exposure to liability should be limited. In order to answer this question, we will first recall the position of the security industry in EU law, international conventions and Member State law in order to ask whether the security industry could, on the basis of this analysis, be exposed to substantial liability risks (8.1.1). The entire discussion concerning the exposure to liability of the security industry obviously takes place in the shadow of “big brother”, the US, and in this particular case the US Safety Act. This merits a question on whether the liability exposure of the security industry in Europe is similar to the liability exposure of the security industry in the US. In addition, the question needs to be asked what can be learnt from the legal analysis of the US Safety Act provided in chapter 7 (8.1.2).

During the course of this study, intense discussions with stakeholders took place. Stakeholders also clearly presented their opinions via different (position) papers arguing in favour of a limitation of liability. The arguments of industry will be discussed in 8.1.3. Next, a specific focus will be provided concerning the tasks of the security industry, also addressing whether the security industry, precisely because it provides security (or at least is supposed to do so) is fundamentally different than other industry sectors to such an extent that it would warrant a different treatment at a policy level (8.1.4). If one were to conclude that this is indeed the case and hence would merit a different treatment of the security industry, i.e. some type of limitation of liability, the question can also be asked whether there may be potential disadvantages of restricting the scope of application of liability rules as far as the security industry is concerned (8.1.5).

From the outset, we should state that, as is often the case with policy debates, on many issues one can have different observations, depending obviously on the particular position one takes within this debate. Within the framework of this project, we see it as our task to present the different arguments from an objective perspective and hence to critically assess the merits of the argument that the security industry is different and merits a different treatment (in the sense of restricting its liability exposure). However, like with many policy discussions, these questions often do not lead to black or white yes/no answers. We therefore aim at providing the different arguments and informing the debate by providing advantages and disadvantages of different options (thus aiding the decision making process at policy level) rather than to take a final stance on those issues ourselves.

8.1.1. Liability exposure of the European security industry de lege lata

First in chapter 3, comparable EU legislation was examined, also in the light of the question to what extent this legislation could be relevant for the security industry. In the summary of chapter 3 we held that theoretically any type of legislation could be relevant for the security industry, but that such would require a rather far-fetched interpretation. Many of the European law sources that were discussed in chapter 3 were qualified as not directly relevant for the security industry.\(^{918}\) This was certainly the case for the Environmental Liability Directive, which does not seem relevant for the security industry’s third party liability.

The Product Liability Directive, on the other hand, is relevant to the extent that security products are indeed defective, i.e. that they do not provide the security that the public in that particular case may expect.\(^{919}\) However, it has to be added that under the Product Liability Directive (PLD) there is no liability for damage to professional property or for pure economic loss. The decision whether there is liability for pain and suffering is left to the Member

---

\(^{918}\) See 3.6.3.
\(^{919}\) See suprax 3.6.3.
States. In addition, the PLD also excludes development risks which may be quite important, given the large uncertainties on techniques e.g. used by terrorists. It was also held that compliance with regulation, such as REACH, may have an influence on liability in the sense that a product is no longer considered defective if it complies with regulation. However, that result largely depends upon the interpretation in national courts. One particular piece of EU legislation, the regulation on insurance requirements for air carriers and aircraft operators, is relevant in the sense that it has a strong effect of channelling (in an economic sense) liability to air carriers and aircraft operators. Since the solvency of aircraft carriers and aircraft operators is guaranteed through the mandatory insurance, victims may have primarily incentives to sue aircraft carriers and aircraft operators whose solvency is guaranteed. This could hence potentially limit the liability exposure of the security industry.

Similar conclusions followed from an analysis of international law treaties dealing with civil aviation, nuclear safety and environmental liability in chapter 5. As was held in the summary the conventions discussed in that chapter are relevant to the extent that they often channel liability to particular operators; in some cases even exclusively. This is e.g. the case in the international convention on civil liability for oil pollution damage (CLC) which channels liability in principle exclusively to the ship owner. Hence, the liability of others (including the security industry) is excluded. Also in cases where involvement of the security industry may be more likely, like in the nuclear area, there is a strong reliance on channelling to the operator of the nuclear power plant. Exceptions to the channelling are quite difficult and would mostly only occur if there were an agreement between say the operator of the nuclear plant and a third party (like the security industry). It is unlikely that the security industry would voluntarily accept liability in case of a nuclear accident. In that sense, it can be held that exclusive channelling to e.g. the operator of a nuclear power plant or a ship owner in fact shields the security industry from liability. In other conventions (e.g. Montreal Convention on International Carriage by Air) the channelling is not exclusive, but the persons who could be held liable are addressed in a limited manner in the convention, e.g. indicating that liability would be possible against other agents of the contracting or actual carrier.

It is equally important to stress that in most international conventions the number of defences and the possibilities to call off them are relatively limited. E.g. in the Rome and Montreal conventions terrorism or natural disasters do not constitute a ground of excuse or justification. Again, this may be reassuring for the security industry since it can mean that the exclusively channelled (strict) liability will apply to the designated operators in the international conventions. That again limits the likelihood that on the basis of those conventions a victim would call on the liability of the security industry. That would only be possible in case of recourse and then only in those conventions that allow for such a recourse.

Summarizing, the study of comparable European legislation in chapter 3 and of liability regimes in the international treaties in chapter 5 do not create a specific liability regime for the security industry. To the contrary, it seems that the exclusive channelling in the international treaties to other parties in fact shields the security industry to a large extent from liability.

However, there could of course still be liability based on national law which was addressed in chapter 4. As the analysis of chapter 4 showed there is first of all no special case in any of the reports mentioned with respect to tort liability of security companies in the analysed jurisdictions. This obviously is a striking finding. According to the national reports in the

---

920 Article 9 PLD.
921 See supra 5.5.2.
922 See supra 4.3.
seven legal systems that were analysed (England and Wales, France, Germany, the Netherlands, Poland, Spain and Sweden) there has never been any case where the security industry was held liable on the basis of tort law. The only case that is mentioned by the reporter for England and Wales does not deal with third party liability but with liability of the security company towards the client based on the contract. The other case reported by the Swedish reporters dealt with the right of recourse of the insurance company against the security company. The Swedish court rejected the claim with the reasoning that the breach of the contractual duties the security company owed to the client does not amount to negligence in tort towards the client’s customers.

The comparative overview makes clear that in particular countries compensation funds have been created for victims of terrorism (France, Spain, UK). Although the scope of those compensation funds in some cases is limited, the mere fact that victims can rely on a compensation fund could potentially limit the liability exposure of the security industry. However, both the French and the Spanish act provide for subrogation which could virtually reach the security industry.

The comparative report provided in chapter 4 makes clear that all of the analysed jurisdictions provide for fault-based liability which would constitute the first legal basis for direct claims of third parties against the security company. The other basis would constitute product liability, either (still existing) national product liability rules or the implementation of the European Product Liability Directive, to which we already referred above.

Fault based liability requires the breach of a duty of care. The security provider who is not the operator of the activity which needs protection, or the tortfeasor who causes the harm in the first place, assumes the duty to provide security only with the conclusion of the security contract with the client. The wording and contents of the contract not only specify the obligations of the security provider with respect to the client, but also shape the potential liability of the security provider towards third parties. The contract, on the one hand, defines the tasks and duties of the security provider and, on the other hand, also circumscribes the group of persons to whom the security provider owes a duty of care. A victim who is part of the protected group may then sue the security provider directly for damages. Not only to the client, but also with respect to third parties the security provider is primarily obliged to fulfil his contractual obligations. He cannot be held liable both by the client or any third party for the mere fact that the stipulated measure, device or security standard does not meet the highest standard provided by the industry. Liability can only arise if the security provider knew or should have known that the security measures are inadequate and if he failed to inform the client of this fact and thus disabled the client from taking adequate measures to prevent the damage. The situation is, however, different if the security provider contractually agrees to secure a facility or an activity in a comprehensive way and independently from particular instructions by the client. In this case the security provider takes over the responsibility for the security of the undertaking from the client and will also assume tort liability towards third persons. In many countries this situation is described by the theory of the liability of the independent contractor.

For the liability of the security provider towards third persons or even the general public it is important to note that the breach of a contractual duty does not in any case amount to tortious behaviour towards third parties. All the seven jurisdictions that were examined in the project provide for specific concepts to restrict the responsibility of the tortfeasor for harm that is not reasonably foreseeable or is too remote to trigger liability. These restrictions play an important role for the liability of the security provider for damage caused by a natural disaster.

923 See supra 4.3.7.2.
or by a terrorist act, as is exemplified in the case studies of chapter 4. These restrictions apply
to all types of damage, but are quite essential for the compensability of pure economic loss
sustained by third parties.

Under extra-contractual liability, compensation for pure economic loss is rather restricted. In
England and Wales, Germany and Sweden pure economic loss is in extra-contractual liability
only recoverable under exceptional circumstances. In the other countries (France,
Netherlands, Poland and Spain) which do not distinguish between pure economic loss and the
other heads of damage in the first place restrict the compensability of pure economic loss by
further considerations, such as the necessity of a sufficiently direct causal link (France, Spain)
or by the concept of adequacy (Poland) or by more general considerations (Netherlands). The
responsibility of the security provider will usually not extend to the compensation of
environmental damage either, such as relief measures of a public entity, preventive measures
by the public authority or remedial action, as the security provider is not liable according to
the Environmental Liability Directive.

In addition, there is a theoretical possibility of an obligation of the security industry towards
the client for an action of recourse. The construction would then be that the client would be
sued directly by the victim (e.g. under a strict liability rule applicable to operators of
dangerous activities) in which case the client could try to execute a recourse to the security
industry. This recourse obligation can either be directly provided by the contract with the
client or it can follow from the fact that both client and security provider are jointly and
severally liable to the victim. In this case the client will have a right of recourse against the
security provider if he compensates the victim. Also in the latter case the recourse between
the client and the security company is subject to the contract concluded between both parties
and can hence be adjusted to the specific circumstances of the case. It would e.g. be
admissible that the client limits or completely renounces his right of recourse against the
security provider. This is in some cases referred to as a so-called “hold harmless” clause,
according to which the security industry would be held “harmless” in the sense that clients
would refrain from exercising recourse on the security industry.924 In this regard it is of
interest that in most countries there will be no recourse obligation of the security provider
when the damage is caused by a natural disaster or a terrorist attack, as such events are in
most countries qualified as ‘force majeure’ or ‘act of god’ and exonerate the client from
liability be it fault-based or strict.

Summarizing: in national law, there are undoubtedly theoretical possibilities, as the country
reports summarized in chapter 4 shows, to hold the security industry liable for damage
incurred by third persons, either on the basis of fault/negligence or on the basis of product
liability. This liability will usually only cover compensation for death, personal injury and
property damage and only very exceptionally pure economic loss and environmental damage
if it does not also constitute property damage. If the damage is caused by a natural disaster or
by an intentional act of a third person, the security provider will only be liable if he had a duty
doing of care to prevent the occurrence of such damage. Even if this is the case liability of the
security provider may be denied by national tort law as the link between the carelessness of
the security provider and the sustained damage may be assessed to being too remote to trigger
liability.

However, the most important conclusion is probably that so far in none of the seven
jurisdictions that were examined there has been any case where the security industry was ever

924 However, during meetings with stakeholders the security industry held that, especially when clients are public
authorities, it may be difficult to insert those clauses into contracts. They claimed that especially as far as public
procurement contracts are concerned, public authorities to the contrary often shift liability to the security industry.
held liable in tort towards a third party. Based on that analysis, it hence seems safe to conclude that at least today liability of the security industry towards third parties is not (yet) a serious problem in Europe.

8.1.2. Comparison with the US

A starting point for this entire project has not only been the fear of the security industry to be exposed to large liabilities in Europe (to which we referred in 8.1.1), but is also related to the fact that in the US since 2002 there is a US Safety Act. In the US, it was hence apparently judged at political level that there was a substantial threat of the security industry which made a deviation from normal tort rules necessary.

We will now come back to the situation in the US and compare it to Europe in two different ways. First, we will point at a few general differences concerning the liability litigation environment in the US and in Europe, arguing that those differences may explain why the exposure of the security industry to liability in the US is more substantial than in Europe (8.1.2.1). Next, we will again come back to chapter 7 where the US Safety Act was discussed and address again the specific reasons for introducing the US Safety Act and addressing the particular remedies provided in that Act in the light of the question whether such an Act would be needed in Europe as well (8.1.2.2). Finally also differences between Europe and the US as far as the functions of tort law are concerned will be discussed (8.1.2.3).

8.1.2.1. The liability litigation environment in the US and Europe

8.1.2.1.1 Introduction

This section examines key aspects of US civil and liability litigation and compares to the European liability litigation environment. Most literature on the subject focuses on substantive law, but there are important differences between US and European civil procedure, and diverging rules on evidence, compensable damages and damage awards. The US is known as a ‘litigious society’ and the causes of the relatively high level of litigation in the US and the sometimes extraordinary results of US liability litigation are explored. This analysis suggests that the basic reason for the wide trans-Atlantic differences lies in these essentially procedural differences.

We survey first differences between the US and European litigation systems. The second part examines in more detail the procedural and other features of the US system. The procedural, evidentiary and related imperfections of the US system are contrasted with the European system. In addition to the enormous damage awards, high litigation and indirect cost, this part addresses the unintended side effects of discovery, admissibility of unsound scientific evidence, pitfalls of decision-making by juries, and the impossibility of proving absence of defect and causation (all of which may influence application of concepts of ‘defect’ and ‘causation’ to sets of specific facts). It explores how these features of the US liability system may help explain the liability crisis in the US. The third part deals with selected substantive law issues, including evidence. The fourth part sets forth the conclusions.

8.1.2.1.2 Summary of differences between US and European liability litigation

This part highlights some of the most salient differences between the two systems. The U.S. litigation system is very different from the civil law liability systems common in continental
Europe. These differences are by no means unique to product liability, but the contrasts are often most strong in this context.

The relevant U.S./European liability differences relate mostly to procedural rules and, to a much lesser extent, substantive law. As to the procedural differences, US civil procedure provides plaintiffs with ample opportunity to obtain documents from defendants through ‘discovery’. The process of discovery permits plaintiffs to obtain copies of any documents ‘or other tangible things’ that are in the defendant’s possession. Even documents and information that will be inadmissible at the trial may be subject to discovery. In civil law systems, discovery is an entirely foreign concept. Courts, not parties, have primary responsibility for fact-gathering and eliciting evidence. If a defendant in liability litigation does not submit documents that the court has identified as relevant or if he does not provide enough information for the plaintiff to go forward with his furnishing of proof, a civil law court, under well-defined conditions, may effectively shift the burden of proof to the defendant. The defendant will then have a strong incentive to produce documents that support his position, since he will lose if he is not able to prove his case.

A second important difference between the U.S. and Europe is the cost of defending a liability law suit. Due to factors such as the enormous volumes of documents ‘discovered’ by the parties, the intensely adversarial nature of proceedings, the large number of actions and procedures available to parties, the detailed civil procedure rules and substantive law, the significant lawyer and expert fees, and the system of contingency fees, the cost of defending a liability law suit in the U.S. exceeds by many times the cost of defending a similar law suit in Europe. Moreover, although European civil procedure rules allow a winning defendant to recover some litigation costs, in the U.S. a defendant who has successfully defended a liability claim may not recover any costs.

Third, in the U.S., experts are used as combat weapons. In a product liability law suit, each party hires his own experts (also known as ‘hired guns’) on the basis of the support the experts provide for his arguments. In Europe, on the other hand, party experts are used much less frequently, and court-appointed experts are the rule. Adversarial use of experts in the U.S. not only imposes significant additional cost, but might also undermine reliability and credibility of scientific evidence in the courtroom. Biased, unsound expert opinions, however, are admissible as evidence, and indeed are frequently relied on by fact-finders in U.S. proceedings. In common law countries the expert is often called an “expert witness” and in continental jurisdictions an “expert”. This is caused by the fact that the former jurisdictions are more adversarial and the latter more non-adversarial.

---

925 In civil law systems, the court has a much greater responsibility for fact-gathering. See Langbein 1995, p. 823.
926 The only limitation is that ‘the information appears reasonably calculated to lead to the discovery of admissible evidence’, Federal Rules of Civil Procedure, Rule 26.
927 Plaintiffs’ lawyers typically do not get paid by the hour, but receive a percentage share (typically in the range of 30%) of the plaintiffs’ award. This in turn drives up the amount of damages awards, as US juries are typically well aware of this practice. A survey found that a US-style contingency fee is generally not permitted in EU Member States, except, subject to strict conditions and only with respect to certain cases, in England and Greece. See Faure, Fernhout and Philipsen 2010.
929 See Langbein 1985, p. 836-41. Pursuant to Rule 703 of the Federal Rules of Civil Procedure, courts have authority to appoint experts, but their actual appointment is a relatively infrequent occurrence. See Notes of Advisory Committee on 1972 Proposed Rules.
930 See Mandel 1999.
Fourth, though liability litigation in Europe is handled by judges who are appointed for life, have a law degree and experience on the bench, in the U.S., juries consisting of laymen decide the critical issues (e.g. the factual issues of whether a product is defective, and caused the plaintiff’s damages). Although jury trials in civil matters may be unknown in Europe, the Seventh Amendment of the U.S. Constitution gives a party in federal proceedings a ‘right of trial by jury’ (most state constitutions follow this example for state-law matters). Under the Federal Rules of Civil Procedure, a plaintiff is entitled to a jury trial on serving on the defendant a demand to that effect. A jury is composed of laymen that are selected at random, not on the basis of legal training or relevant technical expertise. As Rule 1861 of the Federal Rules of Civil Procedure puts it, ‘it is the policy of the United States that all litigants shall have the right to grand and petit juries selected at random from a fair cross section of the community in the district or division wherein the court convenes’.

Fifth, there are trans-Atlantic differences in the level of proof required for a finding of ‘fault’ or ‘defect’. Even where the theoretical tests in the U.S. and Europe are not significantly dissimilar, in U.S. liability litigation, findings of ‘defect’ are not always based on conclusive, persuasive evidence, and may at times appear to be at odds with reason and fairness. Where the test is vague (what may a consumer expect?) or the evidence is mixed but an independent expert finds no basis for a reliable conclusion from such evidence, the jury is not precluded from finding a product ‘defective’, nor from finding a causal link between the defect and the damages. In addition to these differences with respect to procedures and evidence, there are other, less significant differences in the substantive law and the way it is applied.

Lastly, in addition to compensation for monetary damages and pain and suffering, US law permits the award of so-called ‘punitive damages’, which are not compensation for damages incurred, but are rationalized as a ‘fine’ to deter future violations. Such ‘punitive damages’ are not known in European civil litigation. Increasingly, European legal scholars are examining the possibilities to introduce punitive damages into European private law as well. The European Commission, however, recommended that punitive damages in the context of collective redress be prohibited.

8.1.2.1.3 Procedural aspects of the US system

Damage Awards and Litigation Costs
The rules governing damage awards constitute the fuel that drives the US liability machinery. As there are no sound, clear and consistent theories and rules on how to compute compensation for pain and suffering in the US, US damage awards can be disproportional to the harm suffered. Plaintiffs in liability suits sometimes receive extraordinary amounts of money for pain and suffering (up to millions of dollars, where in Europe a hundred thousand

---

932 Federal Rules of Civil Procedure, Rule 38. In the demand, the plaintiff may specify the issues he wishes to have tried by jury. Issues not demanded for trial by jury, if any, are tried by the court, i.e., a judge.
933 Subject only to the voir dire procedure, pursuant to which counsel and the court may question potential jurors as to bias or conflicts.
934 Federal Rules of Civil Procedure, Rule 1861. This rule provides further that ‘all citizens shall have the opportunity to be considered for service on grand and petit juries, and shall have an obligation to serve as jurors when summoned for that purpose’.
935 For a theoretical analysis of the development of U.S. product liability (and other) law, as well as of the consequences, see Epstein 1995, p. 211-45.
936 See in that respect Magnus 2010, pp. 104-107.
937 See e.g. Meurkens and Nordin 2012.
938 Commission recommendation on common principles for injunctive and compensatory redress mechanisms in the Member States concerning violations of rights granted under Union law. C(2013)3539/3.
would be remarkable). Comparative overviews of damage awards in Europe show that compensation for pain and suffering, although showing remarkable differences between European countries, still is relatively low.\textsuperscript{939} In addition, they may be awarded ‘punitive damages’ as a ‘fine’ to deter future violations, not as compensation for any damages actually suffered.\textsuperscript{940} This can add up to tens of millions of dollars to the already substantial awards for material damages and pain and suffering.\textsuperscript{941} Obviously, the prospect of such awards provides both plaintiffs and their lawyers (who typically get at least 30\%) with a strong incentive to initiate litigation or seek huge amounts in settlements. Awards are driven up further by the contingency fee system, under which lawyers are entitled to fees of between 25 and 50\% of the damage awards, as courts (or rather juries) undo the monetary effect of this system for the plaintiffs by increasing awards proportionally.

Damage awards in Europe are of course strictly compensatory, not punitive. As reflected by the term ‘damage’, the purpose of a damage award is to restore the plaintiff to the position he would have been in had the wrongful act not occurred (‘restitutio ad integrum’). Moreover, some types of harm are not compensated for in some European countries. The European directive on liability\textsuperscript{942} does not require compensation for pain and suffering, but leaves to Member States the decision whether such compensation should be available. In any event, punitive damages do not exist, as these are considered criminal, not civil, sanctions. Consequently, damage awards are much lower in Europe than in the US and confined to the material harm suffered by the plaintiff.

Litigation costs also tend to be much higher in the US. In the US system, which does not ordinarily permit winning defendants to recoup attorney fees, litigation costs are driven up by fostering discovery and arguments over a large number of procedural and substantive law issues. The US rule barring recovery of litigation and indirect costs by successful defendants, has resulted in increased litigation and settlements providing for significant payments to claimants even if their claims are wholly unsubstantiated. In complex liability litigation, this problem is exacerbated. In a typical case, massive volumes of documents are discovered and reviewed by the parties, their counsel, the juries and the courts, and a large number of witnesses and experts are deposed, examined and cross-examined. This adds not only to the bills of the law firms handling the case, but causes also significant additional costs (experts, document handlers, witnesses, et cetera). Like attorney fees, these costs cannot ordinarily be recovered by the defendant even if he wins.

As might be expected, the US tort liability system, due to these procedural and substantive rules, has become tremendously expensive. Figure 8.1, compiled by the Tillinghast consulting company from insurance-company data, shows the annual costs of the tort system (just one part of the civil litigation system) as a share of gross national product (GNP) in the period 1946-1991.\textsuperscript{943} More recent estimates put the tort system cost at 1.8\% of GNP (approx. $252 billion a year), but this is only the direct cost. Indirect costs caused by tort litigation include non-legal expenses to comply with the tort system, from document management systems, to executive time involved in depositions and pretrial preparation, and opportunity cost due to

\textsuperscript{939} See Rogers.
\textsuperscript{940} Magnus 2010, p. 108.
\textsuperscript{941} This product liability system produces some perverse and costly incentives. Dan Dobbs described the system as follows: ‘Some kinds of claims offer potential recoveries so great that many people may be induced to assert them, even though the win-rate is very low. But if one out of every ten plaintiffs is able to win such a claim, that means nine out of ten defendants must pay attorney fees and other expenses of suit even though they are entirely innocent. The innocent nine are hostages for the liability of the tenth. The costs to them in money and in life disruption may far exceed the gains to the one plaintiff. I count this a very high cost indeed’. Dobbs 1986, p. 49.
\textsuperscript{943} Cited in Rauch 1995, p. 105 (these figures include not just product liability litigation costs, but other areas as well, such as medical malpractice).
activities foregone because of liability risk. It has been argued that fear of liability causes doctors to engage in defensive medicine, manufacturers to refrain from innovation, and pharmaceutical companies to cut back on R&D, resulting in a total cost to the economy from tort litigation of approx. $900 billion a year, which would be some 6% of GNP.\textsuperscript{944}

Figure 8.1: TORT SYSTEM COST AS A SHARE OF GNP, 1946-1991

One may quibble with these (or any other) statistics, but the basic message is clear: the U.S. tort system is expensive. Kakalika and Pace estimated the total expenditure for the tort litigation in state and federal courts in the US in 1985 to be between $29 and $36 billion. From this total 46\% was paid to plaintiffs as net compensation while the rest was taken up in legal fees, insurance company costs and claim processing.\textsuperscript{945} More recent estimates corroborate these findings. Recent estimates of the administrative costs of claims handling via the tort system hold that those are more than $140,000 per claim and that total expenditures on tort claims nation-wide in the US were $290 billion in 2005 (2.33\% of GBP).\textsuperscript{946} As a result of those problems with the (product) liability litigation system in the US, two prominent scholars have recently, in a leading article in Harvard Law Review, advocated the total abolition of product liability tort law.\textsuperscript{947}

By contrast, litigation and related costs in Europe are much lower, because courts have a much greater responsibility for fact-gathering and there simply is less to argue about as the procedural rules are less detailed and tend to leave more to courts’ discretion. Although the US system lowers the litigation threshold in liability cases by not permitting winning defendants to recoup their costs from the plaintiff, in Europe the litigation threshold is lowered by limiting the costs as such and provision of legal aid to the impecunious. In virtually all European countries, a successful defendant may recover at least some, if not all, of his lawyer’s fees from the plaintiff.\textsuperscript{948} Moreover, contingency fees are not typically permitted in European countries. However, there are considerable differences between the

---

\textsuperscript{944} Ted Frank, “A Stimulus You Can Believe In”, May 29, 2009, available at http://www.american.com/archive/2009/may-2009/a-stimulus-you-can-believe-in.\\textsuperscript{945} Kakalika and Pace 1986.\\textsuperscript{946} See the overview with other interesting data in Van Velthoven 2009, p. 470-471.\\textsuperscript{947} Polinsky and Shavell 2010.\\textsuperscript{948} See Hodges 1993, p. 179. In some European countries, a winning party can also be compensated (at least partially) for the cost of expert opinions.
European countries and there is a (small) tendency towards allowing some result-based remuneration in Europe as well.\(^{949}\)

The Unintended Side-Effects of Discovery

The Federal Rules of Civil Procedure (Rule 26(b)) provide:

Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action . . . . It is not ground for objection that the information sought will be inadmissible at trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.

This extremely broad discovery rule is based on the belief that ‘prior to trial every party to a civil action is entitled to the disclosure of all relevant information in the possession of any person, unless otherwise privileged’.\(^{950}\) This discovery rule was controversial when the Federal Rules of Civil Procedure were adopted in 1938 - and criticisms have continued to this day.

Under these discovery rules, in stark contrast to European practice, litigants in U.S. proceedings can require the other side to produce all non-privileged information that is (in a very broad sense) relevant to the litigation at hand, even where that information would not be admissible evidence at trial. Quite apart from the rule’s intended consequences, this broad discovery rule can have significant cost implications for defendants. For example, when served with a discovery request, a litigant is obliged to comply and cooperate - the litigant will need to vet the requested information to ensure that non-privileged information is not disclosed, and will need to make arrangements for the other side to have access to the information.\(^{951}\) Given that discovery requests can be very vague and all encompassing, this can, in complex litigation, involve substantial commitments of management time and, inevitably, legal fees, and can have disruptive effects on on-going business operations.\(^{952}\)

Typically, a great deal of time and money is spent on what has been called the ‘discovery battle’, where lawyers file motions with the court to compel responses to discovery requests, or to obtain protective orders restricting a litigant’s right to discovery of certain matters. Of course, no matter what the outcome of the litigation, a party cannot recover such costs from the other side.\(^{953}\)

Thus, while the discovery rules have certainly had salutary effects, from the 1970s onward there have been growing criticisms of excessive use or abuse of the discovery powers afforded to litigants. As the U.S. Supreme Court said in 1979: ‘There have been repeated expressions of concern about undue and uncontrolled discovery, and voices from this Court have joined the chorus’.\(^{954}\) Or, as U.S. Supreme Court Justice Lewis Powell\(^{955}\) wrote the

\(^{949}\) See Faure, Fernhout and Philipsen 2010.


\(^{951}\) As part of the wide ranging discovery process, product liability plaintiffs often get to explore all the details of the defendant’s manufacturing processes. As a result, the plaintiff may have access to trade secrets and other confidential, proprietary information of the defendant. That information may become available to the defendant’s competitors, especially if used at trial. Settlements typically contain confidentiality provisions that, among other things, prevent the parties and attorneys from disclosing confidential information learned through the litigation. A settlement, therefore, keeps trade secrets and other proprietary information away from competitors. This feature of the US litigation system thus provides an incentive for settling even unsubstantiated claims.

\(^{952}\) As part of the discovery process, the plaintiff can take extensive pre-trial depositions of corporate officers and employees. The deposition of each witness can easily take several days. That process is expensive in terms of attorney fees, and disruptive to the defendant corporation in terms of lost man-hours and distractions to management.

\(^{953}\) The Federal Rules of Civil Procedure do, however, provide courts with powers to punish, in certain cases, those abusing discovery procedures.

\(^{954}\) Herbert v. Lando, (1979) 441 U.S. 153.
following year: ‘Delay and excessive expense now characterize a large percentage of all civil litigation. The problems arise in significant part, as every judge and litigator knows, from abuse of the discovery procedures available under the Rules’.  

In Europe, discovery is essentially unknown. Disclosure of information and submission of documents is left to the discretion of the parties. In most European countries, a plaintiff in a products liability case may seek a court order requiring the production of a document in the possession of the defendant or a third party, but such an order is at the court’s discretion and the plaintiff must show an overriding interest in the production of the particular document. The lack of a discovery procedure in Europe has been a significant impediment to plaintiffs pursuing product liability claims, and this has contributed to a trend in some European countries for courts, in certain situations, to reverse the burden of proof as to fault or defect.  

‘Scientific’ Evidence  
In U.S. liability litigation, a plaintiff’s lawyer has an incentive to hire ‘experts’ on the basis of the lawyer’s assessment of the support the experts will likely provide to the plaintiff’s case. Conversely, these party-experts have an incentive to submit unsound, selective and biased opinions and unreliable scientific evidence, and the applicable rules allow them to do so. As a result, courts and juries in the U.S. are often not supplied with sound, objective expert opinions.  

While party-experts are the rule in the US, it is more common in Europe for the court, at the plaintiff’s or defendant’s request or on its own volition, to appoint an independent, neutral expert who will be required to answer questions phrased by the court. A court is more likely to do so if any expert opinions submitted by the parties differ or appear to be biased or selective. Court-appointed experts are often chosen from official lists of experts with authority in the local scientific community and experience in reporting to courts on technical matters. Courts are free to, and often do, ignore unsound scientific opinions. Although not binding on the court, the findings of a court-appointed technical expert have a considerable and often decisive influence on the outcome of litigation.  

The US Federal Rules of Evidence, on the other hand, do not, at least not in any significant manner, restrict expert testimony offered by the parties. Rule 702 provides that ‘if scientific technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience training, or education, may testify there to in the form of an opinion or otherwise’. The group of persons that qualify as expert witnesses is defined broadly to include any person with a graduate degree (physicians, chemists, pharmacologists, and so forth), irrespective of that person’s authority or standing in the scientific community. An expert is not required to show that he is a recognized expert, authority or specialist, nor does he need to establish that his opinion represents the scientific consensus on an issue or that his

955 It is worth noting that Justice Powell, before his appointment to the U.S. Supreme Court, practised as a lawyer and served in 1964-65 as president of the American Bar Association (ABA).  
958 Peter Huber uses the term ‘junk science’ to describe such unsound evidence (see Huber 1991). Referring to the ‘science of things that aren’t so’, the author shows how time and again lawyers have used - and the courts have accepted - spurious claim by so-called expert witnesses to win astronomical judgments.  
analytical methods are ‘generally accepted’. Thus, a person that is not considered an expert in the field by his peers, or is unknown to the leaders in the field, may submit his opinion. As Yale Law School professor Don Elliott has observed, ‘[t]he law extends equal dignity to the opinions of charlatans and Nobel Prize winners’. 961

As to the contents of expert opinions, the Federal Rules of Evidence are equally liberal. An opinion may be admissible if it ‘assists’ the fact-finder to understand an issue. This is so even if an opinion is clearly at odds with generally accepted scientific views or if the expert’s method conflicts with generally recognized principles of scientific methodology. As Peter Huber points out, an expert may insist that he alone among experts understands the issues to be tried: ‘He may claim to a new Galileo, a lonely, misunderstood genius who can see wonders that others neither discern nor understand’. 962 These liberal rules have caused a large community of professional experts to emerge. These experts, for a fee, make their services available. 963 They typically advertise their services and work consistently only for one group, either plaintiffs or defendants. They are hired and paid by the parties on the basis of the support their opinions will lend to that party’s position. These experts hence have an incentive to produce data that helps their ‘principal’, and disregard data that does not fit that party’s claims. 964 As a result, opinions proffered by expert witnesses do not necessarily reflect the scientific consensus on an issue, and, indeed, may tend to be misleading, biased, one-sided, or, at least, incomplete. 965 An additional problem in that respect is that some lawyers can be very convincing and persuasive and may execute pressure on the expert to provide testimony on the party who hired him. 966 This is especially problematic in cases where differences of opinion may exist. Lawyers will then often exert an influence upon the expert to favour the position of their client. 967 Also empirical research suggests that there is a problem of biased expert witnesses. In that research, among others, the question was asked to judges and attorneys whether “experts abandon objectivity and become advocates for the side that hired them”. The mean score for the judges answering this question was 3.69 on a scale from 1 (very infrequent) to 5 (very frequent). The mean score for attorneys was 3.72. 968

962 Huber 1991, p. 16.
963 In the words of Mandel: “Money changes everything” and experts constitute no exception to that role”. Mandel 1999, p. 113.
964 Some lawyers have openly admitted that they expect expert witnesses to support their client’s claims, at the expense of objectiveness and impartiality. See Huber 1991, p. 18-19.
965 Federal Judge Jack Weinstein, who has written widely about evidence in general and scientific evidence in particular, has observed that under the current system: “an expert can be found to testify to the truth of almost any factual theory, no matter how frivolous, thus validating the case sufficiently to avoid summary judgment and force the matter to trial. At the trial itself an expert’s testimony can be used to obfuscate what would otherwise be a simple case. The most tenuous factual bases are sufficient to produce firm opinions to a high degree of “medical (or other expert) probability” or even of “certainty.” Juries and judges can be, and sometimes are, misled by the expert-for-hire”. See J. Weinstein, ‘Improving Expert Testimony’, 20 Richmond Law Review (1986), 473 at 482.
966 In the words of Thornton and Ward: “This tends to create strong if sometimes subtle pressure upon the economist to directly or indirectly advocate the position of the side that has hired him”. (Thornton, R. and Ward, J., “The Economics in Tort Litigation”, Journal of Economic Perspectives, vol. 13, 1999, pp. 101 et seq. at 106).
967 According to Mandel: “Lawyers are very persuasive characters. If you’re not prepared for it, you can find yourself saying things you would never say to your colleagues” (Mandel 1999, p. 119).
As Learned Hand, the eminent U.S. judge, observed as early as 1901, adversarial methods of using experts’ opinions are ‘an anomaly fertile of much practical inconvenience’. 969 In Learned Hand’s opinion, adversarial use of experts guarantees distortion as experts strive to satisfy those who have employed them or are straight-jacketed by hypothetical questions and the like.970 In short, the U.S. liability system permits parties to submit biased, selective and unsound ‘scientific’ opinions.971 Once admitted, juries are in a position to consider these opinions in deciding the critical issues in dispute.

Decision-making by jury

The U.S. Constitution creates a right to a trial by jury in federal courts.972 The right to jury trial in civil cases is provided for in most state constitutions as well.973 Although well-established legally, the American reliance on juries has not gone without criticism. As noted by one commentator, ‘complaints about the competence of juries to decide legal disputes, particularly civil disputes, accompanied the development of the jury system in England and have continued through the history of American law up to the present’.974 Some criticisms concern juries’ competence and biases with respect to decisions on liability involving scientific or medical testimony.975 Other criticisms center on juries’ suspected propensities with respect to damage awards.976 As noted, in Europe, unlike the US, liability is handled fully by professional judges without any involvement of a jury.977

A frequent criticism is that juries are led astray by ‘junk science’ or ‘hired gun’ experts, or at the least are confused by scientific and medical testimony involving esoterica beyond the competence of lay persons.978 Professor David Sugarman set forth the issue in Science, the prestigious journal of the American Association for the Advancement of Science.979 Sugarman begins by describing West v. Johnson & Johnson Products,980 a products liability case involving toxic shock syndrome (TSS) resulting from the use of tampons. The jury awarded the plaintiff $500,000 in compensatory and $10 million in punitive damages. The trial judge concluded that the award was excessive and the result of ‘passion and prejudice’

---


970 Judge Hand suggested that an approach relying on ‘boards of experts’ would be far more effective. This board would render authoritative opinions that could be transmitted to juries.

971 This, of course, does not mean that every expert opinion submitted by plaintiffs is unsound. Our point is that both unsound and sound opinions ‘are extended equal dignity’. See further on this point also Faure, M. and Visser, L., “The Role of Experts in Assessing Damages – a Law and Economics Account”, European Journal of Risk Regulation, 2011, 376-396.

972 U.S. Constitution, amend. VII.


977 Magnus 2010, p. 111.

978 See e.g. Huber 1991.

979 Sugarman 1990, p. 823.

because the plaintiff had offered insufficient proof of economic loss and had fully recovered from her illness. The award was reduced to $100,000 in compensatory and $1 million in punitive damages. Taking *West* as an example, Sugarman raised these concerns about the jury’s competence:

Jurors selected at least in part for their ignorance about the topic at hand are asked to decide extremely difficult scientific issues: Was it TSS or was it scarlet fever? Could JJP have discovered TSS before the [Center for Disease Control] did? Would it have done so through better testing and follow-up studies? Should the consumer complaints JJP received have put the company on notice that something serious was afoot? Of course, the jury is aided in the process by the testimony of experts. What that means in practice is that it must resolve a dispute between sophisticated witnesses, whose scientific credibility the jurors are unlikely to accurately appraise.

*West v. JPP* is hardly an isolated instance of this phenomenon. It is repeated in nearly every medical malpractice and product design defect case coming to trial...

Further, with regard to the awarding of damages, studies have revealed that, even after controlling for injuries, juries award significantly more money in cases with corporate (or government) defendants, than they do against individuals. This effect, described variously as the ‘deep pocket’ or ‘corporate identity’ effect, has been interpreted to suggest that juries tend to grant larger awards against defendants with at least the appearance of extensive financial assets (‘deep pockets’), driven perhaps out of some notion of distributive justice. More simply put, the amount awarded may have less to do with the harm suffered by the plaintiff than with the identity of the defendant.

It must be said that juries are not without their defenders. Often such defenders argue that (1) juries serve other important social purposes aside from the role of the fact-finder (e.g., citizen participation in government), and (2) juries are not appreciably worse at dealing with factually and scientifically complex litigation than are judges. While one cannot say that there is an unchallenged consensus that juries are substantially more unpredictable or unreliable fact-finders than judges, it does tax common sense that randomly selected laymen would be as discriminating as professional judges.

### 8.1.2.1.4 Selected substantive law issues

**Defendant’s Burden of Proof and Expanding Liability**

By permitting plaintiff lawyers to present selective and biased expert opinions, the U.S. system has effectively imposed the burden of proving ‘no defect’ and ‘no causation’ on defendants. Where defendants have not been able affirmatively to show the absence of defect or the absence of any causal link, findings in favour of plaintiffs have been made. If a plaintiff through discovery and expert opinions has been able to produce some ‘evidence’ suggesting a defect and a link between this defect and a harm, juries and courts could find in the plaintiff’s favour, unless the defendant shows that there is no defect or causal link. Thus, the defendant effectively bears the burden of proof.

---

981 S. Sugarman, 248 *Science* (1990), 823.
983 In addition to a jury’s predilection to redistribute wealth from defendant’s with perceived ‘deep pockets’, which invariably includes large corporations, local sentiment remains a continuing concern with juries. For example, a New York corporation has to be concerned that a Texas jury will be prejudiced in favour of a Texas plaintiff on both finding liability and assessing a damages award.
Moreover, in liability cases, the traditional tests for ‘defect’ and ‘proximate cause’ have been gradually replaced by a test that centers on increased risk and the control over (and spreading of) such risk.\textsuperscript{984} With the judicial acceptance of new theories, liability has gradually expanded and ‘enterprise liability’ has been established. In a scholarly historical overview, Yale Law professor George Priest identified the three main intellectual foundations of current ‘enterprise liability’:

1. Consumers are in a relatively inferior bargaining position and, therefore, contract law (warranties and disclaimers) is insufficient to protect them;
2. The costs of damages caused by a product should be put on the manufacturer of that product so that the price of the product reflects all costs and the market is able to respond (‘cost internalization’); and
3. The costs of injuries should be borne by enterprises because they are in a much better position to spread the risks through insurance.\textsuperscript{985}

As Priest observes, ‘the unavoidable implication of these three presuppositions of manufacturer power, manufacturer insurance, and cost internalization is absolute liability’, since these presuppositions do not incorporate any conceptual limit. As ‘enterprise liability’ developed, courts eliminated the manufacturer’s defenses of contributory negligence, consumer misuse,\textsuperscript{986} and assumption of risk.\textsuperscript{987} This revolution culminated in the notorious 1982 Beshada decision of the New Jersey Supreme Court,\textsuperscript{988} in which the court found an asbestos manufacturer in breach of its duty to warn of product dangers, although the court conceded that the dangers could not have been known scientifically at the time of the breach.\textsuperscript{989} In short, the manufacturer’s liability was limited only by the concept of causation.\textsuperscript{990} If the product was shown not to be the cause, in other words, if the product did not increase the risk of injury, the manufacturer escapes liability.

In liability cases, determining a causal link often requires scientific knowledge. Since courts and juries do not possess such scientific knowledge, expert testimony is offered to provide the necessary elements for decision-making. Hence, plaintiffs’ expert opinions are designed to justify a finding of causation. ‘The art of junk science is to brush away just enough detail to reach desired conclusions, while preserving enough to maintain an aura of authoritative science’, as Mr. Huber has noted.\textsuperscript{992} Thus, these opinions are cast in terms that are broad enough to leave open the possibility that the product on trial caused the plaintiff’s injury. The reasoning typically goes as follows: ‘some medical devices (or chemicals) may, in some circumstances (or doses), cause certain diseases, therefore this specific medical device (or chemical) may have caused this plaintiff’s disease’. Such a statement could even be made in the face of evidence that this specific medical device probably did not cause this plaintiff’s injury, or is not known to cause such injuries. As fact-finders do find a causal link on the basis of expert opinions stating no more than a possibility, manufacturers effectively bear the burden of proving that their product did not cause the plaintiff’s disease. As this requires

\textsuperscript{984} See, e.g., Calabresi 1970.
\textsuperscript{985} Priest 1985, p. 461.
\textsuperscript{987} See, e.g., Hughes v. Magic Chef, (1980), 288 N.W. 2d 542 (Iowa).
\textsuperscript{988} See, e.g., Laque v. McLean, (1972), 8 Cal. 3d 136, 501 P.2d 1163.
\textsuperscript{990} Priest notes that the notion of liability for breach of a duty with which it was impossible to comply, seem to strain the most basic conceptions of responsibility. Priest 1985, p.525.
\textsuperscript{991} And, in some instances, by the concept of defect.
\textsuperscript{992} Huber 1991, p. 157.
proof of a negative fact, manufacturers often do not succeed in persuading juries and courts.\footnote{Quoting Oliver Wendell Holmes, Huber notes that ‘certitude is not the test of certainty. The best test of certainty we have is good science - the science of publication, replication, and verification, the science of consensus and peer review’. Huber 1991, p. 228.}

In Europe, the burden of proof lies, and often stays, with the plaintiff. Article 4 of the European Directive on Product Liability provides that ‘the injured person shall be required to prove the damage, the defect and the causal relationship between damage and defect’. Thus, in strict product liability litigation under the European Directive, the plaintiff must prove a defect, \textit{i.e.} show that the product did not offer the ‘safety which a person is entitled to expect’. The term ‘person’ does not refer to the general public, nor to each individual consumer, but imposes an objective test.\footnote{L. Schmidt-Salzer and H. Hollmann, \textit{Kommentar EG-Richtlinie Produkthaftung}, (Recht und Wirtschaft, 1986), nr 31-42.} Expert opinion often plays a crucial role in complex cases; but, unlike under the U.S. jury system, the opinions of Nobel Prize winners and charlatans will not be extended equal dignity. National laws may permit courts to shift the burden of proof, but courts (unlike juries) are not likely to do so without credible evidence that there is a defect and a causal link.

The Defect Test
U.S. product liability has been extended to include product features that are inherent to the product (for example, the fact that alcohol causes certain diseases has been considered a ‘defect’ of alcoholic drinks) or are obvious to any normal user (for example, the fact that hot coffee may cause burns if spilled over the body). As noted, the concept of ‘causation’ has been extended to include a statistically increased chance that a certain event will happen, even if no actual, scientific cause has been identified.\footnote{W. Landes and R.A. Posner, ‘Causation in Tort Law: An Economic Approach’, 12 \textit{J. Leg. Stud.} (1983), 109.} Damage awards, however, are not proportionate to the risk increase, but cover the full amount of the damages, thus providing compensation for damages that were not caused by the product.

In design defect cases, the critical issue is whether a product was defectively designed. Products have been found defectively designed because a safer design would have been technically feasible. Such findings have been made without regard to cost implications, risk-utility comparisons and other trade-offs that are inherent to the process of product design. Since there is seldom a simple point of comparison, juries are required to compare real and hypothetical products. Even where the instructions to the jury could be said to do justice to trade-offs inherent in product design, findings of defective design have been made where there was overwhelming evidence of product’s favourable risk-utility ratio. For example, after spending $1.5 million in a single year to defend itself in four different lawsuits against its Copper-7 contraceptive device, which had sales of only $11 million, G.O. Searle and Company discontinued the product, even before it ever lost a lawsuit.\footnote{Kip Viscusi, \textit{Reforming Products Liability}, (Harvard University Press, 1991), 66.} In response to this and other cases, the National Academy of Science in 1990 opined that product liability had put the U.S. a decade behind Europe in the development of contraceptive devices.\footnote{\textit{Ibid.}}

Product Liability Reform
Although there is a strong product liability reform movement in the US, there is much less discussion on this subject in Europe. The European Directive on product liability entered into force in 1985 and the first Commission report on the effects of this Directive has been
The Commission did not see a need to submit any proposals for amendments. Although the directive introduced strict liability in many European countries for the first time, it appears not to have resulted in an increase in the number of cases filed with the courts of EU Member States. Consequently, the number of cases reported to the Commission is very low. It should be noted that some European authors have proposed changes to the liability system at the national level with respect to issues such as contingency fees, causation, punitive damages, pain and suffering, and compensation of emotional harms. Limited reforms have been advocated in the Netherlands, and there is some case law suggesting that courts are willing to entertain new theories. On the other hand, no dramatic changes are expected, and in most European countries there remains strong opposition to features such as punitive damages. A 1992 German Bundesgerichtshof ruling that a US judgment against a German defendant ordering payment of punitive damages did not violate German public policy, for instance, has been severely criticized.

The shortcomings of the U.S. litigation system, however, have not gone unnoticed. For example, various states adopted product liability statutes to alleviate the situation. In 1993, a Product Liability Fairness Bill was submitted to the federal legislature, but never adopted. Over the years, the US Congress considered various other tort reform bill. These proposals have consistently encountered trenchant criticism from the Association of Trial Lawyers of America and other associations of plaintiffs’ lawyers. In the midst of the turmoil, the authoritative American Law Institute (ALI) revised its Restatement of Products Liability. The ALI’s report deals with three main issues: product defectiveness, causation and affirmative defences, but does not address any of the procedure and litigation-related issues. In some states, tort reform legislation has been adopted, with varying degrees of success.

Overall, tort reform has not gone very far. The courts continue to apply the theories developed during the several couple of decades, and awards for compensatory and punitive damages remain very high. The predominant test in US product liability litigation remains the consumer expectations test, in particular in relation to manufacturing and warning defects.

---

1000 See, for example, the theory of ‘no causation liability’ raised in a Dutch DES case, discussed in L. Bergkamp, ‘Compensating Personal Injuries Caused by DES: No Causation Liability in The Netherlands’, European Journal of Health Law 1, (1995), 2.
1002 This bill would have reformed product liability significantly in such areas as the availability of compensatory and punitive damages, the level of proof sufficient for an award of punitive damages, the burden of proof to recover compensatory damages, preemption, alternative dispute resolution, expedited judgments, and the admissibility of evidence of collateral benefits as an offset to compensatory damages. With respect to punitive damages, the bill provided that they are available only (‘if otherwise permitted by applicable law’) to claimants who establish that the harm suffered was ‘the result of conduct manifesting a manufacturer’s or products seller’s conscious, flagrant indifference to the safety of those persons who might be harmed by the product’. The bill would also have set a ‘clear and convincing’ standard for punitive damages, a rule that finds support in some state products liability statutes.
1003 Restatement (third) of torts: products liability (ALI, 1997).
With respect to design defects, the test is somewhat different and turns on ‘reasonable alternative design’. Under the EU Products Liability Directive, a ‘public safety expectation test’ is used to assess defects, but this test is qualified by ‘taking all circumstances into account, including: (a) the presentation of the product; (b) the use to which it could reasonable be expected that the product would be put; [and] (c) the time when the product was put into circulation’.

8.1.2.1.5 Conclusion

Diverging substantive law rules cannot explain the vast differences between US and European civil liability litigation. Indeed, procedural differences examined in this section and the availability of significant awards, rather than substantive law differences, fuel liability litigation in the US. While each of the procedural rules, viewed independently, may have an alluring rationale, their synergy produces extraordinary results.

The main reasons why the US liability system has produced these results is that the set of rules constituting this system is not designed, at reasonable cost, to enhance the system’s ability to distinguish between ‘defective’ and ‘non-defective’ products and services, to determine causal link, and to award appropriate compensation for damages incurred by plaintiffs. The outcomes of product liability law suits are unpredictable. Even if all sound scientific evidence suggests absence of any defect, product liability defendants will incur significant cost in management time and in attorney and expert fees, and will run a risk of having to pay enormous amounts of money in compensatory and so-called ‘punitive’ damages, even though many law suits do not end with substantial awards. The theories used for assessing pain and suffering and punitive damages are all but pragmatic. In the absence of clear and consistent conceptual limits and rules, damage awards have skyrocketed and fail to reflect actual damages incurred by plaintiffs. As damage awards can be as high as a few hundred million dollars and outcomes are unpredictable, the US liability system has been referred to as a ‘lottery’ funded by US industry. As a result, in the US, injured individuals incited by the potentially huge rewards, file a large number of liability cases each year, even where their claims are weak and devoid of evidence of defect or causation.

The number of reported cases in Europe, on the other hand, is extremely low. In addition, attorney fees and other litigation cost in the US are many times the amounts in Europe. Not diverging substantive law provisions, but enormous, by and large unexplained, awards for pain and suffering and punitive damages, high litigation and indirect costs and unpredictable outcomes are at the heart of the US liability system. In Europe, product liability reform advocates have argued in support of contingency fees, punitive damages, increased awards for pain and suffering, and compensation for emotional harms, but their proposals have not been adopted. There are often respectable justifications for each proposed change, taken in isolation, but, as the US liability crisis has shown, the wrong combination of procedural and substantive rules can cause the liability system to go out of control. With an increasing emphasis on ‘victim protection’, moral hazards will increase and plaintiffs will take advantage of a defendant’s more onerous position. As the US experience illustrates, once awards are on the rise, the incentive to sue will become stronger and ‘evidence’ proffered to courts less likely to be objective. As a result, if the decision-makers can be deceived, the outcome of civil liability litigation is more likely to be erroneous (i.e. that compensation is awarded, although there is no fault or defect, no causation, or no damages). The US

---

1004 The Restatement emphasizes that the ‘consumer expectations’ test is ‘not an independent standard for judging the defectiveness of product designs’.

1005 See also supra, section 3.2.1.
experience shows that, if the objectives of consumer protection and compensation are given disproportionate weight at the expense of other important objectives, such as incentives for efficient deterrence, the liability system may derail and produce suboptimal results at excessive cost.

Thus, the US Safety Act cannot be viewed in isolation from the US litigation environment. Any initiative taken at the European level should recognize the different litigation environment in the EU. As a general rule, the EU industry is exposed to a significantly lower level of liability than the US industry. That means that in the EU the need for legislation along the lines of the US Safety Act will be substantially less, if not negligible. That does not necessarily mean, however, that there is no need for an initiative other than legislation; whether there is such a need, is discussed further under 8.7.2., below.

8.1.2.2. The US Safety Act: relevance for Europe

In chapter 7 detailed attention was given to the US Safety Act and after the previous exposé it may now have become clear that this Act should be seen in the light of the liability litigation environment in the US which is completely different than in Europe. We will now turn back to chapter 7 where the US Safety Act was described and point at a few important issues which make it also different from the situation in Europe:

- First, it should be stressed\textsuperscript{1006} that the US Safety Act only passed narrowly in Congress and hence certainly did not have unanimous support. Opponents \textit{inter alia} argued that the Act would provide protection even to sellers who knowingly put anti-terrorism products on the market of which they know that they will not work to keep people safe against an attack.

- The US Safety Act is based on a complicated designation and certification system and hence does not provide a generalized exclusion of liability.

- The Designations will be issued for a reasonable period, but no longer than 36 months; there is hence a sunset clause.

- Most importantly: in the US, there have been (although only few) cases (as chapter 7 indicates) where victims have attempted to hold the security industry liable in third party liability suits.\textsuperscript{1007} As the overview, moreover, shows, in most cases liability of the security industry was denied. It should, also be repeated that those cases have so far been absent in Europe.

- To the contents, the US Safety Act provides a bar against punitive damages. However, as we have explained before, punitive damages are not recoverable in most European legal systems.\textsuperscript{1008}

- The US Safety Act also provides a cap (limit) on liability to an insurable amount. But the European (re)insurance industry argues (as we will explain below) that they have never heard of any insurability problem with the security industry as a result of which that justification could not be used for a similar regulatory action in Europe.

- The US Safety Act also provides exclusive federal jurisdiction (obviously with the goal to restrict the likelihood of too generous damage awards in state courts). This jurisdictional issue does not play in Europe either as victims cannot bring suits in European courts.

\textsuperscript{1006} As was mentioned above in section 7.1.1.

\textsuperscript{1007} See supra 7.2.

\textsuperscript{1008} With the exception of English law, but even there the award of punitive damages is much more restrictive than in the US. See Magnus 2010, p. 106-107.
Finally, the US Safety Act restricts the award of “non-economic damages” (typically pain and suffering) to suits against the seller only in direct proportion to the defendant’s liability for economic harm. In addition, there is a bar against non-economic damages in the absence of physical injury. Again, both measures aim at restricting high amounts for pain and suffering which is, as we have argued above, also one of the typical features of the US liability system in which it differs from tort law in most European legal systems, where the award of high amounts in paying and suffering is not considered as a major problem.\textsuperscript{1009}

In sum, the most important goal of the US Safety Act is to react against typical features of the US liability litigation environment, by imposing a liability cap to an insurable amount (assuming insurability problems for the security industry), imposing a bar on punitive damages and limiting the award of (non-economic) damages (to avoid the imposition of high amounts of payment suffering by juries). To a large extent, these problematic aspects do not exist in the European tort liability environment as a result of which it is doubtful that a similar legislative instrument would be needed in Europe. To a large extent, the US Safety Act provides protection against features of the American liability litigation environment which are absent in Europe.

8.1.2.3. \textit{Function and goal of tort law}

There is one final but important difference between the use of tort law in the US and in Europe which should be discussed. This concerns the fact that most victims in Western Europe, contrary to their American counterparts, do not have many incentives to bring a liability suit, since the social security system in many western European countries provides for a relatively wide coverage of many expenses that a victim incurs when an accident happens. Partially as a result of international conventions\textsuperscript{1010} and European directives, many countries have elaborated systems of compulsory first party insurance covering medical expenses. In addition, lost income is often taken care of as well. Depending upon the legal system, this is usually mandatory if one is employed and on a voluntary basis for self-employed individuals. In some cases, even property losses are insured, depending upon the type of accident. This relatively elaborated first party insurance system has as a consequence that a large part of the damage to the victim in European legal systems is already taken care of. This means that victims in Europe often do not have incentives to sue an injurer in tort. Their only incentive to use the tort system is for the part of the damage that was not taken care of via the first party or social security insurance scheme. This could be in some cases for property loss, or for the higher part of one’s income which could not be compensated and for pain and suffering for which first party insurance is usually not available. In addition, the social insurance carriers could execute recourse against liable tort feasors or their insurers.

As a consequence of this system, many victims in Europe do not use the tort system even if they could. This considers especially individuals with lower or average income who are compensated via social insurance schemes and who do not wish to use the tort system for pain and suffering. Moreover, social insurance carriers \textit{de facto} rarely use their right to exercise recourse, \textit{inter alia} because exercising that right creates relatively high administrative costs. For victims in European legal systems tort law is hence often considered as a “luxury” system since it provides full compensation and the luxury of also compensating the top of one’s

\textsuperscript{1009} See also Faure and Hartlief 1996, p. 265-266.
\textsuperscript{1010} See in that respect e.g. the European Social Charter of 18 October 1961 and the ILO-Convention No. 24 concerning sickness insurance for workers in industry and commerce and domestic servants, No. 25 concerning sickness insurance for agricultural workers and No. 102 concerning minimum standards of social security.
income and pain and suffering. However, the majority of victims in Europe may never use the tort system and will simply stick to the awards received via the social insurance schemes. In that sense some have qualified tort law as a luxury system that, at least in the European context, is not used for “Existenzsicherung”. For “Existenzsicherung” victims in European legal systems can call on social security and social insurance schemes.

The situation in the US is of course completely different where, in addition to Medicaid and Medicare and some workmen’s compensation schemes, many tort victims cannot benefit to the same extent as in Europe from generalized social security schemes. Hence, as a consequence victims in the US will (have to) use the tort system also to obtain compensation of their primary needs (medical expenses and lost income) whereas that is largely covered by social security and social insurance schemes in Europe. That hence creates fundamental differences between the need to call on tort law for victims in the US and in Europe. Whereas in the US using tort law for many victims is a matter of survival and receiving compensation of basic needs, in Europe, the tort system is (given the existence of social security) rather a “luxury”. That fundamental difference of course explains that the exposure of the (security) industry in the US to liability suits is potentially much larger than in Europe.

8.1.3. Industry stakeholders positions on limitation of liability of the security industry

In position papers and otherwise, security industry-related trade associations have advocated EU action to limit their potential liability exposure in connection with the supply of goods and services. The concerns expressed by the industry focus on the risks of terrorist attacks (and similar acts of aggression), and the large scale damage that may result therefrom. In the post-9/11 era, the US adopted the Safety Act, which is considered a success in making liability predictable and eliminating unlimited exposure, and thereby stimulating innovation. The security industry argues that the EU should likewise take action to address the unlimited liability issue.

To better understand the industry’s positions, the project team met with representatives of trade associations and companies. These interviews were conducted on the basis of a questionnaire that the project team developed specifically for this purpose; this questionnaire also requests that respondents submit any relevant written documents. All respondents, but one, provided oral responses to some or all of the questions; we received one written response to the questionnaire. In addition, one stakeholder supplied a document entitled “Third Party Liability Limitation, Preliminary Legal Study” (Final Draft, March 2010), which, as its subtitle suggests, purports to discuss “the main laws and cases relating to the liability and compensation for damages suffered by victims of acts of terrorism in Europe,” and was prepared “in support of the proposal for the adoption of an EU legislation on third part liability limiting the exposure of the industries in case of damages caused by acts of terrorism.” Because this is the only document (other than the position papers and the written questionnaire response) provided to the study team by security industry representatives in support of the case for liability limitation, we have analyzed it in some detail. These are the main conclusions we reached:

- Although this paper presents conclusions and arguments, it does not provide any references to European case law nor does it analyze the scope of the security industry’s liability exposure; the paper provides some basic analysis of liability laws of Denmark, France, Germany, Italy, and the United Kingdom, but when it arrives at

---

1011 See Faure and Hartlief (1996), 254-261. Even where victims benefit from certain social security benefits, the tort liability system provides strong incentives to initiate litigation.
“Case law on acts of terrorism,” for each of these Member States except Denmark (which was treated only cursorily), the paper notes “Further research is to be made on possible cases where security manufacturers or service providers are found liable in [Member State] courts for failure of a product/service.”

- The paper states that “[t]he legal risks consist in the exposure (specifically of the security industry but also of other public or private entities involved in the protection of activities against acts of terrorism) to claims brought by a great number of victims for an overall significant amount of damages. In fact, an act of terrorism can cause an accident that is normally remote in terms of probability but potentially entailing massive harms and costs for multiple targets.” The paper does not provide facts or analysis supporting this statement. It is revealing, however, because it suggests that the industry’s position is based on perceived exposure, or fear of liability, rather than on actual liability exposure.

- Further, the industry does not believe that its third party liability exposure can be limited by contract, where the paper states as follows:

> “The mitigation of the legal risks cannot be obtained by contract. In general, contractual provisions may distribute the financial burden between the parties to the contract (e.g. to which extent a part is to be held harmless and indemnified by the other part and how the payments should be made to third parties), but they are not enforceable in all circumstances vis-à-vis third parties (e.g. disclaimers or limitations of liability do not apply to third parties and claims can validly be brought by the victims for the total amount of damages against whoever can be held liable by a judge).”

The paper does not provide a basis for this concern. It should be noted too that the paper does not state that security providers are unable to negotiate liability limitations with their customers; as discussed below, this argument came up in position papers and discussions with security industry representatives.

- Remarkably, the paper is even skeptical of the enforceability of the EU-wide liability limitation advocated by the industry, where it states as follows:

> “Even assuming that a satisfactory agreement can be reached on the liability limitation at EU level, its enforceability needs to be checked in the light of the fundamental principles of law that are applicable at national level. A specific review of legislation and case law concerning similar mandatory limitations in the field of tort law is necessary. In particular, lines of decisions in national courts may consider the cap unenforceable in case of gross negligence or wilful misconduct of the supplier and/or in case the limitation does not allow a sufficient protection to the victims considering all circumstances. In certain Member States, the provision of security products or services may be qualified as a dangerous activity, subject to a strict liability regime without any limitation ceiling.”

Again, the paper may be indicative of unfounded fears that circulate within the security industry. We recognize, however, that the industry paper is labeled a ‘preliminary study’ and that there may be other arguments and facts that provide support for industry positions. The observation that the United States legislature enacted the Safety Act without extensive empirical analysis of the effects of liability exposure on the security industry, may have shaped the expectations of the industry in the EU.
In this section, we summarize the industry position, noting where opinions diverge. To this end, we used the position papers published by European associations, the summaries of the interviews, and the written response to the questionnaire.

We met with representatives of the following associations and companies (for more details, see Annex 2):

- CoESS: Confederation of European Security Services
- ASSA-I: Aviation Security Services Association International
- ASD: AeroSpace and Defence Industries Association of Europe
- EOS: European Organisation for Security
- GIFAS: French aerospace industries association
- ACI: Airports Council International Europe
- Euralarm: Association of the European Fire and Security Industry
- AmCham EU: American Chamber of Commerce to the EU
- Safran
- Boeing

The summary below discusses first the information provided in relation to perceived liability exposure and the arguments relating thereto, then the information regarding insurance, and finally the proposed solutions. The proposed solutions identify the specific associations that advocate it. Most of the arguments advanced are shared by more than one (but not all) association and/or company (they are not necessarily identified each time).

8.1.3.1. Liability exposure of the security industry

The ability of the security industry, like other businesses, to predict and mitigate its liability has long been a concern. After the attack of September 11, 2001, however, the concern for liability in the security industry was significantly heightened. Lawsuits brought against airlines, security contractors, airport operators and an aviation stakeholder - which at some point involved claims for some $20 billion - are still pending in US courts. The unusual nature of the attack and the magnitude of the damages, as well as the aggressive nature of the allegations in the lawsuits underscored the need for predictable, stable liability protection. The industry lost confidence in insurance to adequately mitigate liability when insurance companies stopped insuring against terrorism risks for years afterwards.

According to some interviewees, the main driver is the persistent threat of terrorist attacks coupled with the changes in the insurance market following 9/11. They emphasized that the need for effective and innovative security technologies has never been more critical. But the traditional risk-mitigator for the development and diffusion of such technologies - insurance - is now inadequate. The insurance market changed dramatically after 9/11: exclusions or severe limitations were added to most policies for terrorist events. More than ten years afterwards, stakeholders have asserted that adequate and viable insurance for acts of terrorism continues to be unavailable. The limits continue to be too low to cover the risk and even when

insurance is available in a given year, there is no certainty concerning its continued availability. Security technologies operate for years, while insurance policies are generally renewable annually. Thus, when insurance practices change, as they did after 9/11, manufacturers and operators of deployed security technologies can become exposed. This risk, interviewees claims, discourages them from developing and deploying such technologies.

According to interviewees, terrorism can create the extreme example of the kind of liability the security industry faces on any given day. Some notable examples they provided, are the following:

9/11: The security claims in the WTC event against the security companies and the airlines centered on the failure of their detection equipment, security personnel, and procedures to detect the weapons of the hijackers and their suspicious demeanor/ID's. The security claims against an aviation stakeholder were as follows: (a) the cockpit doors were of insufficient strength to withstand hostile intrusion; (b) the hijackers were able to turn off the transponder; (c) there was no system, such as password-protection, that prevented the hijackers from turning off the autopilot system or operating the flight controls; (d) there was no system that automatically notified the government or the airline that an unauthorized pilot was at the controls; (e) the flight management computer could be programmed to fly the aircraft to potential terrorist targets; (f) there was no video surveillance system that would have alerted the pilots to the hijacking; and (g) there was no system that took over control of the aircraft and prevented the terrorists from flying the airplane into the buildings. After 9/11, enhanced cockpit doors were certified under the Safety Act as Anti-Terrorism Technologies (ATT).

It is noteworthy that one of the security company defendants in the massive 9/11 litigation- Huntleigh- paid out so much in claims that they completely exhausted their insurance limits ($500 million). Without the provision in the 9/11 Federal legislation limiting damages awards to available insurance, Huntleigh would be insolvent.

Aircraft Bombings: The bombing of the Pan Am 747 over Lockerbie, Scotland, in 1988 killed 270 persons. The security claim in Pan Am Lockerbie was that Pan Am failed to detect the bomb in the luggage and loaded the luggage even though there was no accompanying passenger. Pan Am was forced to defend against hundreds of wrongful death claims in the US. This tragedy has been universally seen as causing the downfall of Pan Am, once the largest international air carrier in the world. Other more recent examples are the firebombing of the China Northern aircraft in 2002 and the bombing of two Russian airliners in 2004.

Aircraft Shootdowns: The Soviets shot down a KAL 747 passenger plane in 1983. 269 passengers and crew were killed. The aircraft inadvertently flew into Soviet airspace. The crew was cited for failure to properly navigate to avoid intrusion into the hostile airspace. As to KAL, the claims against the airline included a mix of security and poor navigation. Security in the sense that protection of the aircraft from hostile attack depended on careful navigation, particularly with the route chosen by the airline that came so close to Russian air space. Poor navigation was claimed with respect to the navigation of this particular flight. The airline was sued in hundreds of claims in the US (Wash D.C.) and paid many millions in settlement.

Aircraft Hijackings: There have been at least 18 hijackings of airliners since 2000. Many have occurred since 9/11, particularly outside the US.

World Trade Center Bombing: Prior to 9/11, in 1993, the New York World Trade Center buildings suffered a terrorist bomb explosion that did massive damage. The Port Authority was sued for hundreds of millions in damages and lost in the trial court and the court of appeal. They finally avoided liability just last year when New York State's highest court
reversed the decision, but did so solely on the ground of governmental immunity. That defense would not have been available to a nongovernmental entity.

**School, Theater and Mall Shootings:** The tragic shootings at Columbine, Virginia Tech and other schools have resulted in claims against school districts for inadequate security. The Aurora Colorado theater killings and other shopping mall attacks have similarly resulted in inadequate security claims against the security companies and property owners. The media and experts have deemed such lawsuits "inevitable".

**Other Nonterrorist SI liability examples:** SI providers are frequent targets by claimants in the US in a wide variety of situations. Failures of burglar alarms, fire alarms, smoke detectors, carbon monoxide detectors, anti-hacking software, and radiation detectors are but a few examples. It is the norm in the US that an SI provider will be sued if damages result from a security breach.

**EU Product Liability:** While the litigation climate is different in the US than in the EU, the EU has become more litigious. For instance, there has recently been discussion within the EU to adopt US-style class action rights and procedures. In fact, US class action law firms were set up in Europe following the Madrid and London terrorist attacks. Damages awards have been increasing as well. See below for a summary of average awards for aviation liability claims, which was submitted to the study team to show that European average awards have been trending upward in recent years (source: Marsh, a global leader in insurance broking and risk management). Note that the numbers, which were supplied by a security industry representative, lump Canada and the Europe together; it is hence not possible to deduct an upward trend only for Europe from this information.

**Table: Average Liability Award**

<table>
<thead>
<tr>
<th>Region</th>
<th>10 Year</th>
<th>3 Year</th>
<th>3 Year</th>
<th>Largest</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>7,404,002</td>
<td>7,242,000</td>
<td>7,404,000</td>
<td>7,404,000</td>
<td>2009</td>
</tr>
<tr>
<td>Europe &amp; Canada</td>
<td>1,285,017</td>
<td>1,641,002</td>
<td>2,023,442</td>
<td>3,205,402</td>
<td>2009</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>490,730</td>
<td>581,000</td>
<td>951,071</td>
<td>2,584,229</td>
<td>1997</td>
</tr>
<tr>
<td>China</td>
<td>414,900</td>
<td>700,000</td>
<td>750,000</td>
<td>750,000</td>
<td>2010</td>
</tr>
<tr>
<td>Latin America</td>
<td>1,232,080</td>
<td>1,595,910</td>
<td>666,100</td>
<td>2,396,151</td>
<td>2007</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>633,700</td>
<td>605,907</td>
<td>912,514</td>
<td>1,753,700</td>
<td>2005</td>
</tr>
</tbody>
</table>

\(^{1013}\) In the table and figures presented here, Europe and Canada are presented in the same category.
Finally, according to interviewees, in products liability, there has been a trend away from a negligence-based regime towards a strict liability approach, in which the manufacturer may be held liable regardless of fault.

The Institute for the Analysis of Global Security estimates that the 9/11 attacks caused over $100 billion in personal, property, and direct economic damage. Already, insurers have paid out over $40 billion in claims for such losses. The US Government has paid another $9 billion in compensation to individual victims. And litigation continues, with remaining victims and property owners - and insurers as subrogees - still pursuing tens of billions of dollars in further claims of personal, property, and direct economic loss. As security industry representatives assert, there have been many such judgments. Here are some examples of verdicts/settlements involving security claims that have been provided to us:

- $1.8 million verdict last month against Hilton Embassy Suites and SecurAmerica for insufficient security that allegedly resulted in a fatal carjacking;
- $1.8 million settlement for a case against a security company arising from an allegedly faulty home alarm when a woman was murdered in her bedroom;
- $19+ million verdict in 1995 against Pan Am for one of the deaths caused by the Lockerbie bombing. Plaintiff alleged that the airline failed to take effective action after being warned by a co-defendant security company;
- $3.6 million verdict in 1999 against landowners arising from a rape and assault in a university apartment complex. Plaintiffs alleged that the landowners failed to take steps recommended by a security consultant and a security company they hired;
- $2.8 million verdict in 1991 against TWA for a death caused by a bombing of an airplane while it was on the ground in Egypt;

---

1014 Stakeholder response to Questionnaire in Annex II.
- $1.3 million settlement in 2006 for claim against a retail store and a security company for a rape and murder in a store parking lot;
- $600K verdict in 2011 against ADT Security in a breach-of-warranty claim brought by a jewellery store that was later robbed.

Security industry providers have tried to negotiate protection from their government customers, but customers often resist providing protection. Even if indemnity is granted, there needs to be sufficient confidence that it would be enforceable and that the customer has the assets or insurance to render it meaningful. It is claimed that customers are increasingly unwilling to provide any exoneration or indemnity, also since they may face the same inability to insure that exposure as the SI provider. If the customer is a governmental entity, indemnities may be unobtainable or unenforceable as a matter of law or practice.

Further, interviewees point out that through the deployment of high technology, public/private partnerships and the outsourcing of security-related services, the front-line task of protecting citizens worldwide has increasingly fallen on private sector providers of security technologies and services.1015 These providers, unlike other industries, face the continuous risk of their products and services being undermined by terrorists for political or other purposes1016, terrorist attacks are mostly aimed at governments, and are heavily influenced by government politics.

Although the setting of standards of safety and detection remains a government responsibility, interviewees assert that the exposure of security providers to liability in case of a catastrophic terrorist attack is potentially unlimited. This liability bears no relation to the value of the product or service provided and could thus be enterprise-threatening.1017

Security industry representatives point out that governments have reacted in different ways to assure that the victims of terrorist incidents are appropriately compensated and that industry continues to invest and deploy new technologies to protect against the creation of new victims. In Germany, for instance, security services always fall under the umbrella of responsibility of the government so there is no issue. Other countries such as the UK, the Netherlands, and to a lesser degree France, have not only transferred operations but also liability to the industry. Security providers are only a part of the security chain and the current risks of third party liability that they face are disproportionate to their responsibility. Other schemes exist, although many states within and outside the EU have not as yet addressed the issue. In cases where protection is available, it is generally restricted to incidents occurring within the territory of the nation concerned. A market distortion therefore exists, favoring technology and service providers doing business in those protected markets.

The security services industry argues that it is in a very large majority of cases obliged to sign contracts imposing liabilities that go far beyond possible and available insurance coverage. A private subcontractor responsible for carrying out certain specific security tasks in accordance with instructions from authorities and clients and in line with applicable regulations cannot reasonably assume the full risks of all the perils and calamities generated by a possible terrorist attack, the argument seems to go.

---

1016 AmCham EU position on Industrial Policy for the Security Industry, February 2012, p. 3.
1017 Third Part Liability Limitation, Preliminary Legal Study on the main laws and cases relating to the liability and compensation for damages suffered by victims of acts of terrorism in Europe’, March 2010, p. 4.
The French aerospace industry representative sees less need for a limitation of liability. France currently has a regime for compensation of victims that is based on compensation for bodily injury of victims by the Guarantee Fund for the victims of acts of terrorism (“FGTI”), and compensation by insurance companies for damages to property.

8.1.3.2. Liability insurance

Security industry providers claim that, post-9/11, they have limited insurance available with respect to a terrorist attack, via the “Extended Coverage Endorsement (Aviation Liabilities)”, commonly referred to in the insurance industry as the AVN52 writeback. This endorsement provides, typically, $50 million to $250 million in annual aggregate coverage for 6 of the so-called war risks and allied perils, including “any act of one or more persons, whether or not agents of a sovereign power, for political or terrorist purposes and whether the loss or damage resulting therefrom is accidental or intentional.” Excess policies for third party war risks liability are available, but at lower levels than prior to 9/11.

According to some stakeholders, this coverage falls well short of what limits were available pre-9/11, typically full policy limits for third parties. Those limits exceeded $2 billion at the time and coverage was non-cancellable. Now, the war risks and allied perils coverage can be cancelled with 7 days’ notice by the insurers (or 48 hours for certain events).

Even limits of $2 billion or more would be insufficient to cover the claims arising out of a massive terrorist attack. In addition, if an attack occurred, insurers would likely cancel war risks coverage with 7 days’ notice, and the aviation stakeholder would be massively exposed—its products would still be in the marketplace and it would have no insurance coverage.

Stakeholders point out that after 9/11, war risks coverage (which includes terrorism insurance) was greatly scaled back. Third-party limits of $50 million were the norm. For most insured’s, the limit has been increased to $150 million since then, and some insured’s have $250 million in coverage. War risks coverage continues to be available at relatively low levels, but its continued availability is uncertain from year to year. A terrorism incident in any given year will likely cause insurance companies to cancel current coverage and decline to renew terrorism policies the following year, and would expose a security provider to enterprise-threatening risk due to the massive legacy of its products in the marketplace.

In short, industry representatives from the security - and security services industry, as well as airports and airlines face the same problem, i.e. it is impossible for the insurance market to provide for instruments that provide adequate coverage. The insurance market does not offer a solution that would be sufficient to meet the potentially unlimited exposure that could follow from a new terrorist attack.

8.1.3.3. Proposed solutions

In general, the solutions proposed by the security industry focus on liability exposure and insurance, and regulation insofar as it can reduce liability exposure. The representatives of the security industry that participated in this study, however, disagree on the nature of any problem, if any exists, and whether a third party liability limitation for the sole benefit of the security industry is appropriate and necessary.

- EOS and ASD
According to EOS and ASD, private sector providers of security technologies and services for use in the EU need to be given appropriate limitation of liability exposure in order to protect their overall sustainability. The proposed EU legislative act should be limited to acts of terrorism as defined under the Council Framework Decision of 13 June 2002 on Combatting Terrorism. The scope of the proposed act should further be restricted to those security services and technologies that meet set criteria for quality and efficacy. The Member State in which an incident has occurred should be the place of exclusive jurisdiction for any legal complaints. EOS and ASD in summary request a three part model that consists of (1) the security technology or service being accredited through an applicable national accreditation scheme in each jurisdiction where it is to be sold (2) the occurrence of a terrorist incident based on the definition in the Council Framework Decision of 13 June 2002 and (3) a limitation of liability from claims where a terrorist incident has occurred and a security services or technology is alleged to have failed to perform as anticipated.

The EU industry does not necessarily want a duplicate of the US Safety Act in Europe. To implement the US approach the EU would need capacity to approve and certify. In the current economic climate, the appetite for new EU structures and extra administrative levels on EU level is probably very limited. Additionally, it would also need quality control of the product, which is currently imposed at Member State level.

- **CoEss and ASSA-I**

According to CoEss and ASSA-I, solutions must be found that limit liability to levels that are reasonable and/or that provide alternative funding sources of liabilities as existing already in other industries such as the civil nuclear industry. Another solution would be to create a new fund which could be financed by the industry and/or by the national governments.

The EU must work toward legislation aimed at:

- Stating the shared responsibilities when private security is concerned
- Determining the specific responsibility of each stakeholder involved in security
- Limiting the responsibility/liability of private security providers
- Establishing a mechanism for handling third party claims
- Thus eliminating the risk for private security providers of unlimited third party liability

- **GIFAS**

According to GIFAS, French industry is not in favor of a legislative change except regarding certification. GIFAS believes that there is a good balance between liability of the product and solidarity thought the FGTI which compensates victims. Only the state of the art clause is a problem from a French perspective because some judges will always rule against the industry. Therefore, it would be better to have an assumption that when there is certification, the industry is not liable.

- **Aviation stakeholder**

According to an aviation stakeholder, the EU should be encouraged to consider and develop a legislative framework that incentivizes the development and deployment of anti-terrorism technologies for the protection of European citizens. The front-line task of protecting citizens in the EU increasingly falls on private sector providers. The point is that the lack of comparable liability protection hampers the investment, development, sale and installation of security technologies in Europe. The security sector needs special consideration as, unlike other industries, it faces the continuous risk of its products and services being undermined by
terrorists. In addition, risks in those industries are largely insurable, where terrorism risks largely are not. Suppliers of security technologies and services are not looking for an exemption from their due responsibilities, but for a system that will protect them from enterprise threatening risks so that they will develop and deploy innovative technologies to help protect the public.

To ensure a level playing field, the EU should support the development of the best technologies to keep citizens safe, and avoid legal uncertainty and costly law suits for determining the applicable jurisdiction. The EU should consider the adoption of a Regulation. A solution would indeed be best achieved from an EU perspective, rather than at Member States’ level, so to ensure a European free and fair security market which does not distort competition.

- **ACI**

ACI does not object to an instrument based on the Safety Act if there is no doubt that the governments hold final responsibility and that states take responsibility for damages above a certain threshold. A security act with a limitation of responsibility for the security industry should not lead to an increased exposure for airports. A security act is only desirable if it is recognized that airports act as agent of the state in providing security services and that the state will pay for amounts above a certain limit. Further, in international conventions security is always provided for under the umbrella of government responsibility. The main problem of a potential security act from their point of view is the insecurity behind it.

ACI is in favor of a security act that limits responsibility and where the state takes up liability claims above a certain amount. This is written down in international conventions and the current practice everywhere else in the world. Until now, no State has clearly stated whether airports were in fact liable, it is the interpretation of civil aviation agencies. A formal recognition in a formal text is desirable since the current situation with no official interpretation of the rules makes it unclear what a government will do once a terrorist attack has actually occurred.

- **Euralarm**

According to Euralarm, any solution should cover both products and services, as both are always interconnected. This solution should build on existing certifications rather than creating an additional layer. Existing certifications could, for example, include further assessment, such as assessment conducted under the US Safety Act.

The alarm industry is facing different approaches in various Member States. A solution should thus preferably be adopted at the EU level to ensure consistency and a level playing field. This solution could be operated either at the EU level (eg, via a new or existing body) or at the national level (e.g., Member States would grant limited liability under national law based on criteria developed at the EU level).

- **AmCham EU**

AmCham EU fully supports the policy proposal that EOS and ASD have developed. This proposed legislative act would acknowledge an obligatory third party liability within the EU for all security technology and service providers up to a defined liability cap. Below such a cap, the security technology or service providers will retain the risk of a potential liability or, alternatively, will transfer it to an insurer (if available) for a premium.
As current national procedures and requirements contribute to trade barriers among Member States, the Commission should consider and promote certification/conformity schemes for all security products. Via Commission mandates to European standards organizations should lead to step-by-step, end-user driven standardization based on the evaluation of existing national, European and international standards. New standards must be technology-neutral and be based on the desired outcomes and performance of complete systems, rather than the capabilities of individual technologies since technology specific approaches may lead to freezing development and deter further investment in alternative technologies.

According to AmCham, the EU and US should cooperate more closely in the hopes of a system of mutual recognition of certification and testing standards at the very least, and possibly to the adoption of joint standards.

In the current situation, contractors are disincentivized (and thus unlikely) to invest in technology areas where they cannot capitalize on those investments via downstream opportunities, where threat of liability risk causes them to avoid or abandon the risk-bearing markets. This loss of investment will have corresponding effect on availability of both ready solutions and the skills and expertise in associated areas.

AmCham points out that before the Safety Act was enacted in the US, government contractors became increasingly unwilling to accept the potentially enterprise-threatening risk of developing and deploying anti-terrorism technologies and to bid for related contracts. This self-screening due to liability not only negatively affects the contractors but the commercial and government customers as well. It limits the pool of otherwise-qualified bidders, reducing competition and choice of cost-effective best-value solutions for the buyer. Also, as mentioned above, self-screening opportunities based on liability also results in a disincentive for industry to invest in security technologies in those areas, leading to a reduction or elimination of investments and a corresponding loss of innovation and technology readiness for deployment. In short, companies have declined to pursue business opportunities because of liability concerns.

8.1.3.4. Summary

From this overview of arguments provided by the different stakeholders, it first of all appears that their interests and opinions differ. E.g. where many plead in favour of an exclusion or limitation of liability, arguing that there would be a problematic liability exposure, others, more particularly the French Aerospace Industry, do not see a need for a limitation of liability. Some stakeholders are concerned about liability limitations if these result in increased liability exposure for other operators; for instance, the Airport Council International has doubts about a possible EU Security Act and pleads in favour of compensation via the state. Notwithstanding these differences, there are some general points mentioned by the stakeholders that can be summarized as follows:

- Many argue that there are (in the US) many terrorist and other attacks where either the liability of the security industry was involved or could be involved. At the same time, stakeholders also point at increasing amounts of damage awards.
- It is also held that the security industry de facto provides safety which in fact remains a government responsibility. That also makes the position of the security industry different than the position of other industries.
- It is held that (in the US) liability insurance cover for terrorism would not be available or only for low amounts and that even the limits of $2 billion would be an insufficient liability cover.
- It is also held that contractual liability exclusions with clients are often impossible, especially in cases where clients would be government (related).
As a solution, some stakeholders propose:
- Exclusion of liability for incidents related to terrorism;
- A financial limit (cap) for other types of damage above which government should intervene.

We will weigh and discuss these arguments of the stakeholders in the next section where a few policy observations are formulated concerning the specific position of the security industry.\textsuperscript{1018} In concluding this section, we should note also that the security industry representatives that participated in the study, despite our repeated explicit requests (including, but not limited to, a written request to supply “any information (…) relating to [the liability exposure of security goods and/or services providers], including legal analysis, legal opinions, studies on the effects of perceived liability risks, case law, etc.”), have not provided any relevant documentary evidence to support their assertions. For example, the study team received no documents backing up the claims relating to “enterprise-threatening” liability exposure, the unavailability of insurance and the contractual obligations imposed on security providers by public authorities. To the contrary, as discussed above, the only substantive analysis that the study team received from these representatives, was incomplete, provided only some very basic information about the liability regimes of some Member States, and did not support these representatives’ arguments about the industry’s third party liability exposure, the unavailability of insurance, or the onerous contractual obligations imposed on security providers.

8.1.4. Policy observations

As discussed in Chapter 2, the security industry is composed of providers of goods and services intended to prevent terrorist attacks and similar acts of aggression at (i) facilities such as airports and train stations, (ii) means of transport such as airplanes and trains, and (iii) critical infrastructure such as petrochemical refineries and nuclear power plants. The range of products is wide and ranges from detection equipment to surveillance cameras. Services include guarding and security services, as well and maintenance of equipment and security consultancy services.

The analysis of the EU and national liability law (see Chapters 3 and 4) shows that the security industry, to some extent, is exposed to potential liabilities for large scale damage, for instance, in connection with terrorist attacks involving airplane crashes into buildings such as those that happened in the US on September 11, 2001 (“9/11”).\textsuperscript{1019} Although there have been no cases in Europe of the same scale as the US litigation following ‘9/11’ and despite the absence of any sound analysis of the security industry’s liability risks in Europe, security industry representatives have asked for EU intervention that would limit its liability exposure.

The liability laws applying to the security industry are general and cover all other sectors of industry, such as software companies, pharmaceutical companies and accountants. To the extent that the services and goods supplied by these companies create a risk of large scale damage, they are likewise exposed to potentially huge liabilities.

This raises the question why only the security industry would be entitled to a special liability limitation. How is the security industry different from these other sectors of industry? In other

\textsuperscript{1018}See 8.1.4.5.
\textsuperscript{1019}As we concluded before (see also 8.1.1) it will probably not be the European legislation that would constitute the basis for the liability of the security industry. However, based on the national legal systems (discussed in chapter 4) it can (even though there have not been any cases yet) not be excluded that the security industry would be held liable on the basis of national tort law towards third parties.
words, do we need to think differently about the liability exposure of the security industry, and, if so, in what sense are they in a different position?

For purposes of this study, we need to consider whether the security industry is unique and different from other sectors of industry with respect to (1) exposure to civil liabilities, and (2) ability to deploy risk mitigation mechanisms. As discussed below, it has been claimed that the first factor coupled with the second would render the security industry particularly vulnerable to extreme unlimited civil liability exposure. These arguments, if they are supported by the facts, would therefore point in the direction of the specific situation and tasks of the security industry, which, in turn, might argue in favour of treating the security industry differently, also as far as the exposure to liability is concerned. In discussing the merits of this argument, we also discuss the actual extent of the industry’s liability exposure, a few potentially problematic issues associated with a liability limitation and whether there truly is an insurability problem, as is claimed by the security industry. This will enable us to critically weigh the arguments presented by the stakeholders and provide a summary of the arguments in favour and against limiting the liability exposure of the security industry.

8.1.4.1. The security industry’s potential liability exposure

The analysis presented in previous chapters and the arguments made by stakeholders suggest that the factors set forth below cause the security industry’s liability exposure to be potentially larger than the liability exposure of other sectors of industry. Note that the arguments articulated below have not been made by security industry representatives in the terms as they are presented below; they reflect the study team’s analysis and are intended to put forward the strongest case for the security industry in light of the facts and findings of this study. Below, we provide the argument first, followed by some preliminary remarks to put it into context:

1. There are people in society, terrorists and other aggressors, that are intentionally and actively using their best efforts to “beat” security products and services in an attempt to cause massive damage. If they are successful, they show incidentally, given the low frequency of terrorist attacks, that the design of these products can be improved (and, thus, may be defective). This is different from risks that are “passive” in relation to the products that are aimed at limiting them (e.g. bacteria are not intentionally and actively trying to circumvent the effect of an antibiotic). It may be similar, however, to hackers and people that design viruses, worms, trojan horses, and the like, who also try to “beat” system security; the difference is that the nature of the direct damage these cyber-criminals can cause is different from the physical damage that terrorist can cause. Although this argument has some appeal, it should be noted that the security industry specializes in providing protection against security risks, and, as such, specifically addresses the risks of terrorism. Clearly, the argument would be strong, if the standard of liability applicable to security providers were to ignore this aspect

2. For security reasons, security products providers cannot (and are not permitted to) disclose the detection (or other) limits of their products to the general public (as opposed to their customers). If they were to disclose the technical and other limits of their products, they would make it easier for terrorists to circumvent security measures and threaten security. Yet, to limit their potential liability exposure, they would have to provide accurate and complete information on their products. Not providing such information, thus, could be regarded as negligent or as an informational/warning defect. In this respect, a security product may be comparable to a “placebo” in medicine:” it works only if the information about it is incomplete or even deliberately misleading. This argument is correct as far as it goes; it assumes that security providers need to disclose the limits of their
technologies to the general public to limit their third party liability exposure. As discussed below, this study found no evidence, however, that there is any such need.

3. The customers of the security industry, not the security providers themselves, decide which goods and services are procured to secure buildings, installations, and people. Thus, the type of equipment and the nature and level of the services provided are not within the control of the security provider. In deciding which equipment and services to purchase, the security industry’s customers do not aim only at increasing security; they weigh the anticipated costs and benefits of additional or more expensive equipment and services at the margin. For instance, in the context of airport security, better and more powerful screening equipment and services may come at a higher price and also increase waiting and/or clearance time at screening points; an airport may therefore rationally decide to purchase somewhat less powerful equipment and a lower level of service, which is not only cheaper but also reduces waiting and clearance time. Although this argument is correct, it assumes that security providers could be held liable for decisions made by their customers. As discussed below, this study found no evidence of such exposure.

4. Terrorists are generally attacking a state or fighting the government, not the security product provider or the airport, airline, or other facility concerned. Terrorist attacks have nothing to do with the security product/service or the provider. Put differently, the government, by abolishing or changing its policies, decisions and acts, is in the best position to reduce the chance of terrorist attacks. Terrorism is indeed often specifically addressed against governments. Government may therefore also be in the best position to take risk reduction measures and follow adaptation strategies as far as the prevention of terrorism related risk is concerned. The goal of terrorist attacks is often to disrupt society and terrorists may adopt adaptive strategies to which governments can potentially react better than the security industry.\(^{1020}\) Prevention of terrorism in that sense is a public good which should primarily be provided by government and not by private citizens. Conversely, security providers cannot do anything to reduce the “attractiveness” of a target; they can only reduce the chance that the target can be reached. Given that all security products and services can be beaten, circumvented, or rendered ineffective if enough resources are spent on the effort, there is only so much the security industry can do. This argument suggests that the security industry should not be exposed to strict liability for damages caused by terrorists; it does not suggest, however, that third party liability based on fault (or negligence) necessarily raises any issue.

5. Precisely because the security industry often intervenes to help government fulfil its task of providing national security (i.e. prevention of terrorism) the question could even be asked whether the arguments which are sometimes advanced in the literature in favour of state immunity from liability should be extended to the security industry as well. Some have held that public authorities should be considered as a so-called multi-task agency which forces it to balance various external costs against each other. Such a balancing exercise may be extremely difficult and even if the agency performs the exercise with optimal care, it is possible that a court will \textit{ex post} disagree with the decision of the agency. That is according to some an argument for a higher threshold for liability for those so-

\(^{1020}\) See Bruggeman, Faure and Heldt 2012, p. 205-206.
called multi-tasking agents. Uncertainty may have a strong chilling effect on a multi-task agent because the multi-task agent does not internalize the precaution costs.\textsuperscript{1021} It is doubtful, however, whether this argument can be extended to the security industry. After all, the public authority is undoubtedly a multi-tasking agent, having to balance various external costs, but the same is not true for the security industry which executes, as a private commercial party specialized in providing security, a task for the public authority.

6. Neither the security providers nor their customers are necessarily free to determine how they design their products, what products they provide, and which security measures are imposed. In some settings, such as airport security, security providers must comply with highly specific rules that may even specify the equipment to be used (including sensitivity). As noted above, the security industry’s customers pay for the products and services, and they decide how much they will spend on security, which always involves trading off cost and inconvenience against increased security. Civil liability exposure is based on the concept that, as a result of the financial incentives created by liability, providers will take efficient prevention measures. To be able to do so, however, they must be free to decide what measures to take. If they are not free to do so, this would potentially be an argument supporting a liability limitation, assuming the standard of liability is not sufficiently flexible to accommodate this level of complexity. If the government decides what security products and measures are to be used, an argument could be made that the liability for any damages caused by less than perfect security should be imposed on the state, not on the security industry or others (as discussed below, this is, in fact, what the national liability laws of the Member States analyzed in this study, provide). A similar argument could be made with respect to the customers that decide what security products and services they buy and deploy, if better products and services were available but found to be too expensive. This, of course, also raises the issue of who will be ‘holding the bag,’ which is a tricky issue. In any event, the analysis of the liability laws of the Member States does not confirm that there is a significant potential problem with security providers being held liable for decisions made by others, or that the standard of liability ignores legal and regulatory requirements.

8.1.4.2. The security industry’s ability to deploy risk mitigation strategies

The analysis presented in previous chapters and the security industry’s arguments suggest also that, when compared to other sectors, the security industry has more limited ability to deploy risk mitigation measures to limit its liability. This would be so for the following reasons.

1. Security providers have been unable to obtain contractual limitation of their liability. Contractual liability limitations can involve (i) narrow descriptions of primary obligations, limited representations and warranties, (ii) exoneration for certain types of damages, for all damage caused by negligence, or for other types of exposure, (iii) liability limitations in the form of caps or similar mechanisms, (iv) indemnities, and (v) hybrid provisions, combinations of or variations on the above. The customers of the security industry have been able to impose their

\textsuperscript{1021} See De Geest 2012. This is e.g. the case if a public servant needs to decide whether a firm should get a permit or not to carry out a risky activity that can cause substantial harm to third parties.
terms and conditions on their customers, which has resulted in a lack of contractual protection for security providers.

2. As a related matter, the customers of the security industry are often public or semi-public authorities, which buy security products and services through a regulated public procurement process. This may mean that these customers impose their terms and conditions, which tend to favour them, and that non-acceptance of such terms may disqualify the bidder. Where this is so, security industry members either have to accept no limits on their potential liability or they cannot bid on the projects. On economic and business reasons, security companies may not want to forego this market and will therefore accept the terms offered.

3. The security industry holds that it has not been able to contract adequate insurance at reasonable price to cover the liability risks associated with terrorist acts. As a result, so the security companies hold, they are not insured for the liability exposure associated with terrorist attacks.

Beyond these considerations, there are also broader public policy issues associated with civil liability exposure of the security industry. For instance, should we encourage innovation in security, and if so, should we do so through liability limitations? Having hence identified two lines of reasoning showing that the security industry may be different than other industries, we will now analyze these arguments in light of the security industry’s actual liability exposure, and examine whether there really is an insurability problem as argued by the security industry. We also look at a few potential disadvantages of a limitation of the security industry.

8.1.4.3. Issues with contracting for liability limitations and insurability?

- Contracting for liability limitations:

The industry representatives have asserted (without providing documentary evidence) that security providers are unable to negotiate limitations on their liability in contracts with the Member State’s public authorities and governmental agencies. In other words, these Member State public authorities insist that security providers remain fully liable under the applicable law. The security industry representatives argue that there are always bidders that are willing to accept these onerous conditions, and that, in some cases, individual companies decide not to participate in bidding processes, because they are not willing to assume the liability risks. They do not assert, however, that they are exposed to competitors that offer sub-standard products or services or have limited assets, except in the area of maritime security, where it is claimed that some non-EU competitors receive financial guarantees from their home governments.

If it were the case that financially strong security providers offering high quality products/services are consistently losing business (due to their reluctance to accept unlimited liability risks) to financially weak providers offering sub-standard products/services, this would be a concern. It would not justify a liability limitation, however; rather, it would possibly provide an argument in favor of regulation of security providers, or another measure targeting the financially weak companies.

In the absence of problems of underdeterrence of financially weak companies (and the ‘judgment-proof’ problem), if and to the extent that security providers are ‘forced’ to accept contract that do not provide for any limits on their liability, such contract clauses could be viewed as merely reflecting the preferences of the Member States governments. Viewed as
such, it is hard to see how the EU could take effective action. The EU would have a difficult
time supporting contractual liability protection for the security industry, because that would
appear to go diametrically against the Member State governments’ explicit preferences for
full liability exposure of security providers.

The alleged practice of the Member States’ public authorities to refuse to grant liability
limitations could be consistent with a well functioning market. The same is true for any
practice of security providers to decide, based on the totality of their liability exposure,
whether they will bid for a specific project. The study team has not been supplied with any
documentary evidence of a structural problem or competition distortion. If there is no
structural problem, the market may just be competitive in relation to ability and willingness to
assume liability risks; in that case, a liability limitation would eliminate competition and
encourage excessive risk-taking.

- Insurability:

Written questionnaire responses and other information were received from a large reinsurer
and a European insurance association. Both were asked whether the liability exposure of the
security industry in Europe would justify a limitation of liability for the European security
industry in a similar way as it had been done in the US; the question was also asked whether
they are aware of insurability problems for the security industry.

The representatives from a large reinsurer declared that they were not aware of specific
problems concerning the insurability of the security industry. Until today they never heard
that there would be any problem with the insurability of the security industry. Normally
reinsurers would, for example through their national insurance associations, hear when a
particular industry has difficulties in obtaining cover. They would normally then try to find
particular solutions.

Of course, the respondents realize that in the US there are particular problems that have to be
addressed there. Moreover, it is argued that every line of business, not only the security
industry, but for example also the petrochemical industry, has its own particular risks. It is not
clear why, from an insurance perspective, the security industry would be different.

The risk that, for example, the security industry would be held liable in Europe in relation to
terrorism at airports, is assessed as being relatively small. Moreover, to the extent that the risk
would exist, it is not considered as uninsurable. There are coverages available, and in liability
insurance terrorism risk is covered as well.

If an incident would cause billions of euros of damage, there may obviously be an insurability
problem, as insurance capacity is never unlimited. But respondents from the reinsurer never
heard of a problem of limited capacity and other industries would potentially be exposed to
those high risks as well.

It is emphasized that for the terrorism risk particular pools have been created. In Germany,
Extremus has been created for the terrorism risk. This would mostly be attractive for airports,
but many airports do not even take insurance cover. They decide this on a yearly basis. Some
years they prefer to run the risk instead of paying (relatively high) premiums. Hence,
according to the representatives of the reinsurer, also the airports consider the risk of a
terrorism attack relatively limited as a consequence of which they are not willing to pay high

\[ ^{1022} \text{Interview held on 12 March 2013.} \]
\[ ^{1023} \text{See supra 6.3.5.} \]
premiums to Extremus. Note that this is representative only for Germany. The case may be different if one is located e.g. on Knightsbridge in London which could potentially be more vulnerable to terrorism attacks. Those pool solutions for terrorism exist everywhere and there is no lack of capacity. Larger installations, such as a big airport, may have to pay a yearly premium to cover the terrorism risk of 1 million euro or more. That explains why in some years they may purchase cover and in other years not. This shows that even the primary subjects exposed to the terrorism risk (the airports) do not consider the risk so high that they always seek insurance coverage. This raises the question why the risk would be higher for more remote parties like the security industry? For them, a criterion would be whether there is an actual need with the security industry. Such an actual need was there with the first party terrorism risk after 9/11 as a result of which pooling solutions were created. However, the reinsurer was not aware of a particular need as far as the security industry is concerned.

Victims will obviously try to go after the deep pockets. Hence they may go after e.g. a big airport (in case an incident would occur there) or obviously after the state. But most security companies are not such deep pockets that they would have to fear unjustified liability suits on that basis alone. Moreover, in reality they would only have to fear liability suits when there is liability cover available. Then they would become a deep pocket as a result of which the liability risk would increase.

It is also stressed that the security industry itself is created to provide security against terrorism-related risks to third parties. Hence, it would be strange that when precisely these risks would materialize for which they are responsible, they would be shielded from liability.

Respondents also see a general problem with the attitude of the security industry in that if one starts with allowing exceptions, then any type of industry could come by and claim that they are exposed to high risks. For example, mobile phone producers could argue that if in the future it would appear that certain radiation from the mobile phones would cause damage, they could go out of business as a result of which mobile phones would no longer be produced. Also, the legal basis on which one could claim against the security industry is relatively limited. Usually, it would be product liability and, as is well known, in Europe the development risk is basically excluded (only very few countries included it).

A somewhat similar picture was provided through information provided by the European insurance association. This association indicates that the picture strongly depends upon the Member State involved. They also hold that a distinction should be made between security products and security services. Security products can fall under the EU Product Liability Directive which assigns strict liability for defective products and which can be covered through product liability insurance. Services would, however, not fall under product liability insurance. The individual market availabilities of insurers vary according to the Member States involved. In some countries (such as Denmark and the UK), it is held that insurance covering the security industry against terrorism-related risks is available in the markets. The same would be the case for Germany. However, in other countries, such as in Central and Eastern European Member States (more particularly Slovenia), terrorism would often be excluded from liability policies. They therefore conclude that the market availability throughout the EU varies.

1024 Ibidem.
1025 Ibidem.
1026 E-mail exchange with insurance association.
8.1.4.4. Analysis of issues

One has to keep in mind that on the one hand, as we discussed above, arguments can be made to argue that the security industry would be in a different position than other industries in Europe, if, in fact, there is potential increased liability exposure and a limited ability to deploy risk mitigation strategies. However, even if these problems can be shown to be real, one should be careful to deduce from them that this would warrant a limitation of liability. In that respect, we should recall the fundamental goals of a liability system, as they were also outlined above. A liability system aims at prevention and deterrence, as well as at an adequate risk allocation and loss spreading. If the liability of a particular operator (in this case the security industry) were limited, an unavoidable consequence is that the goals of the liability system cannot be reached to the same extent. Specifically, this would mean:

- An exclusion or limitation of liability of security providers would imply that liability’s preventive and deterrent effect would be reduced. Exposure to liability has the desirable effect of providing the security industry with incentives to take preventive measures. If liability were to be excluded or limited, there would hence be a price to pay for society in terms of reduced incentives of the security industry towards prevention. (The argument of one industry representative that the industry will do the right things irrespective of any liability threat (and that to suggest otherwise is to ‘insult’ the industry), does not help the case for a liability limitation; if the argument were true, it would simply suggest that liability is not a problem at all.)
- A consequence would equally be that risk allocation would change. Not being exposed to the same level of liability, the security industry would purchase less insurance or other financial guarantees to cover its liability as a result of which its relative prices would be too low. Limitations or exclusions of liability in that sense constitute a subsidy and have as a consequence that market prices no longer reflect the full social costs of the activity.
- From a distributional/loss spreading perspective, a limitation or exclusion of liability always has as a consequence that liability law can no longer exercise its loss-spreading function to the same extent. That may be problematic to the extent that losses can no longer be spread and would remain with the victim (or would require the establishment of another loss-spreading mechanism). Hence, when considering a possible limitation strategy, one should always weigh the advantages of a limitation against the disadvantages in terms of reduced prevention incentives or changed distributional consequences.

There is another issue at the policy level if a special treatment (in the sense of limiting liability) for the security industry were deemed desirable. That has to do with the fact that at the legislative level one would have to define “the security industry”. We devoted an entire chapter (chapter 2) to providing a working definition of the security industry and, for the purposes of our study we finally came up with a definition that is narrower than for example broader definitions used in the EC Communication with respect to the security industrial policy. We made clear that we provided this narrower definition merely for the purposes of the research within this project. However, if the EU were to decide to provide a special liability protection to the security industry, an unavoidable issue is that a clear definition would have to be formulated that could also be used at the legislative level. Not only would a choice have to be made on whether the security industry only includes products or also services, but also to which branches it would extend. The example of the US Safety Act illustrates this difficulty. In the US, the problem, to some extent, was solved via a certification

---

1028 Discussed in chapter 7.
system as a result of which only companies that qualify for this specific certification will enjoy the protection under the US Safety Act.

At this stage, we only want to point at the fact that providing an accurate definition of the security industry, and hence of the scope of protection of a specific legislative instrument will be a difficulty that the legislature will be confronted with in the drafting process.

8.1.4.5. Assessing stakeholders’ arguments

In light of the information provided by the insurance representatives and the discussion of liability’s objectives above, we now come back to the arguments presented earlier by the stakeholders to support a limitation of liability.

1. Security industry representatives argued that, generally, there is a high liability exposure of the security industry (8.1.3.1). In addition, it was mentioned that liability is generally expanding and that damage awards are increasing as well.

These arguments are supported, however, by examples coming from the US. As discussed in chapter 4, thus far, in Europe, there are no cases in which the security industry has been held liable for damages suffered by a third party victim, and security providers can limit their liability exposure by contract, as the contractual standard will also play a role in defining the standard of third party liability. Second, incidents (terrorist attacks and product liability cases) are mentioned, which resulted in the US in liability suits against operators, but not in all cases (successfully) against the security industry. Third, in this respect we should also refer to the comparison with the US provided above\textsuperscript{1029} where we clearly indicated that the liability litigation environment in the US is completely different from litigation in Europe. Hence, the many examples provided from the US are not necessarily indicative of the liability exposure of the European security industry. Likewise, the analysis of the national liability laws presented in chapter 4 does not confirm that the security industry is exposed to liability risks that are comparable to the risks in the US. Where international treaties provide for liability caps, they do so only in the context of strict liability, not fault liability.

2. The argument was made that the security industry is different from other industries, since the security industry provides security, which is normally the government responsibility.

In general, it is the government that assumes responsibility for public security (e.g., the police force is a part of the government). The government, however, may want private parties to perform private and public security functions, also where terrorism is concerned. As discussed, a limitation of the liability of government (being a multi-tasking agent that has to weigh conflicting policy objectives) for public security may be justified, but the same rationale does not necessarily apply to the security industry. Security providers remain private entities specifically specializing in providing security and can hence not automatically invoke the same arguments that would justify governmental immunity.

3. The argument is also made that there would be insufficient liability insurance available for the security industry, especially as far as terrorism is concerned.

In this respect, again, many of the arguments, especially referring to the amounts, are based on the situation in the US, not on the European situation. E.g. the argument that $2 billion

\textsuperscript{1029} See 8.1.2.
may be insufficient coverage for the security industry can undoubtedly be correct, given damage awards in the US. It is, however, doubtful that those arguments apply to the situation in Europe as well. The representatives of the security industry that participated in the study have not provided any documentary evidence of their asserted inability to contract insurance, so the veracity of this argument could not be evaluated by the study team. However, the information provided by the insurance representatives suggests that insurance against terrorism-related risks is not generally unavailable, although it will be subject to a financial limit and terms and conditions, and the situation may vary across the EU.

Specifically, as the reinsurer that was interviewed stressed (and as we discussed in detail in chapter 6), as far as terrorism is concerned, governments and insurers have together worked out alternatives in order to provide cover for terrorism-related risk by government providing an additional risk layer.\textsuperscript{1030} Hence, in almost all European legal systems for first party (damage) insurance, governments and the insurance world have reacted adequately by creating specific facilities to make terrorism-related risks again insurable, after the initial setback after 9/11. That terrorism would still be generally uninsurable is, as a result of those special facilities, no longer the case, although the situation may differ from Member State to Member State, as one insurance association emphasized. Moreover, as the comparative analysis has shown,\textsuperscript{1031} some legal systems (like France and Spain) have created special funds for the compensation of victims (at least for personal injury) in case of terrorist attacks. Hence, in such cases, victim compensation would in Europe primarily take place either via the specific facilities (such as Extremus in Germany) or via the compensation funds (in France and Spain).

Finally, the summary of our interview with a large reinsurer speaks for itself: one of the largest reinsurers in the world is apparently of the opinion that today there is no structural problem with the cover of the liability of the security industry, at least in Europe. The response by an European insurance association provides a similar picture, although it is held that availability of insurance cover varies among the Member States. Further, the reinsurer suggests that, to the extent that liability cover were a problem in some Member States, the security industry could work with the (re)insurance industry to devise specific solutions to cover catastrophic risks, rather than argue for a limitation of its liability.

4. The fourth argument presented by the security industry was that it is difficult for them to exclude liability via contract.

This is the argument that mitigation strategies are difficult, which we discussed above.\textsuperscript{1032} The security industry’s representatives that participated in the study, however, have not supplied any documentary evidence to support this argument. As far as public procurement is concerned and for government contracts, as discussed above, to the extent security providers have a hard time negotiating liability limitations and indemnities, this may simply reflect the preferences of the Member State governments. Since EU measures require the backing of the Member States, it is not plausible that they would support a measure limiting the security industry’s liability because such a measure would conflict with their policies in respect of public procurement of security goods and services. In this respect we can also refer to the opinion of the large reinsurer that one may wonder whether the difficulties of one particular sector (the security industry) to negotiate adequate contracts with “hold-harmless” clauses with its contracting partners are a good reason for shifting risks to others (the public at large or the insurance industry).

\textsuperscript{1030} See supra 6.3.5.
\textsuperscript{1031} See 4.3.
\textsuperscript{1032} See 8.1.4.2.
8.1.4.6. Summary

Although each individual factor discussed above may not place the security industry in a unique position with respect to its liability exposure, it is possible that the combination of the factors is unique to the security industry. For instance, software companies are potentially exposed to catastrophic liabilities, but they are able to limit their exposure by contract and to contract insurance.

The combination of the exposure to large liabilities (even where it is based solely on fault) and the inability to limit such exposure by contract (although insurance, by definition, is subject to financial limits) might render the security industry uniquely vulnerable to catastrophic liabilities. That does not mean, however, that therefore liability exposure must be directly limited. It may mean that there possibly is exceptional liability exposure that may require policy makers’ attention. This study, however, does not provide support for urgent measures.

In addressing the specific liability situation of the security industry it is equally important not only to look at the specific difficulties that the security industry may undoubtedly be confronted with. At a policy level, attention should also be paid at the fundamental goals of a liability system, realizing that those goals may be endangered when liability exposure is excluded or limited. There must hence be important policy reasons to justify such an exclusion or limitation of liability, given the potentially negative effects of such a measure as far as deterrence (prevention), risk allocation and loss spreading are concerned. Moreover, the policy maker should also realize that some of the arguments presented by the security industry in favour of such a limitation of liability take the liability exposure of the security industry in the US as a starting point, insufficiently recognizing that the liability litigation environment in Europe is completely different from the US. Moreover, in the decision-making at the policy level it should also be taken into account that in most EU Member States specific solutions have been worked out to cover damage resulting from terroristic activities; the large reinsurer that was interviewed by us said not to be aware of any problem as far as the insurability of the liability of the security industry in Europe is concerned. This cautions against adoption of any measures leading to an exclusion or limitation of the liability of the security industry.

8.2. Options to limit liability

If the policy makers were to conclude that the security industry does need separate treatment as far as liability law is concerned, the next question would be what the various ways are to limit liability exposure. In theory, there are many options. In this section, we will present several ways of limiting liability exposure and discuss the pros and cons of the various options. The fact that we present these options does not mean that we recommend that the EU should adopt any of these measures.

8.2.1. Limiting compensation to particular heads of damage

One first option is not to provide a generalized liability cap (i.e. a general limit on the compensation due to the victim, but to limit the particular types of damages that could be compensated, thus excluding other types of damage). Particular examples of that were found in the European legislation discussed in chapter 3. For example, the Environmental Liability Directive is limited to damage to protected species and habitats, water damage and land
damage; traditional damage, such as damage to health and property, has been excluded. Also under the Product Liability Directive, compensable damage is limited to personal injury and to damage to property. Interestingly, in the debate concerning auditor’s liability it was held that especially economic losses and wrong assessment of damages were important reasons for a larger liability exposure of auditors. In some Member States, there are also limitations with respect to the compensation for so called ‘pure economic loss. In England and Wales, Germany and Sweden pure economic loss is only recoverable under exceptional circumstances in extra-contractual liability. The other countries (France, Netherlands, Poland and Spain) do not distinguish between pure economic loss and the other heads of damages in the first place, but restrict the compensability of pure economic loss by further deliberations, such as the necessity of a sufficiently direct causal link (France, Spain) or by the concept of adequacy (Poland) or by more general deliberations (Netherlands). Are these examples reasons to limit the liability of the security industry to particular heads of damages? Several observations can be made in that respect:

1. The mere fact that in the Product Liability Directive and the Environmental Liability Directive compensation is limited to particular heads of damage does not mean that it was the intention of the (European) legislature that other heads of damage would not be compensable. In fact, this has more to do with the European decision making process as a result of which Member States in the Council agreed to include particular heads of damages in these directives; whether other heads of damage would also be compensable was left to the Member States, without any intention to suggest that those heads of damages should not be compensable.

2. Looking at the situation in the Member States, personal injury and property losses are generally compensable. Only with respect to pure economic loss important limitations already exist in most Member States, either explicitly or via the causation requirement. Liability for pure economic loss is a major concern of the security industry. Given the already existing limits to liability exposure for such losses, specific European action in this respect would not add much to what Member States already have in place.

3. As noted before, there are substantial differences between the US and European liability litigation environments. The fear that particular heads of damage can lead to high compensation (e.g. pain and suffering) may be problematic in the US, but not necessarily in Europe. From that perspective, looking at current practice in European Member States, there is not a strong reason to exclude particular heads, with the possible exception of pure economic loss in some Member States, from compensable damages all together.

4. Finally, excluding particular heads of damage (e.g. pure economic loss) inevitably adversely affects the realisation of the goals of liability law. In the absence of very good reasons for doing so, it is hard to see why particular heads of damage should be entirely excluded as a category of compensable damages.

8.2.2. Liability capping schemes

When referring to liability capping schemes, one can distinguish between different types of liability limitations. One is the possibility for the security provider, also referred to in the comparative analysis, to limit or exclude its liability vis à vis the client (and, indirectly, also third parties) by contract. In freely negotiated contracts the exposure to liability is normally

---

1033 See supra 3.4.
1034 See supra 8.1.2.
1035 See supra 8.1.4.4.
reflected in the price that parties agree upon. This is a well-known application of the so called ‘Coase theorem’. To the extent that parties would agree, for example, that a security industry provider cannot be held liable by the customer and that the customer holds the security industry harmless against claims by third parties, this would, according to a normal economic logic, be reflected in the price agreed upon by the parties. In other words, the price is a reflection of the agreement concerning risk allocation between the parties. A higher price for the security services would in that respect normally correspond with a risk premium paid for the liability of the security provider. The Coase theorem holds that within these contractual situations increased risks can be passed on via the price mechanism.

Whether these possibilities can always be pursued in practice is another issue. There may be, as we mentioned above, limited possibilities for the security industry in practice to negotiate risk mitigation with customers, especially where the client is a public authority that awards the contract via public procurement. However, if parties agree via contract to limit or exclude liability that is, between the parties, in principle possible and enforceable. The national law analysis summarized in Chapter 4 has shown that such limitations, in general, are also given effect vis-à-vis third parties. In addition, if the customer agrees to hold the security provider harmless against third party claims, the liability risk is shifted by the security provider to the customer.

The liability capping schemes we refer to here include the schemes that are found in international treaties on civil aviation, nuclear safety and environmental liability, extensively discussed in chapter 5. As the conclusions of chapter 5 show, in fact, in six of the seven international treaties that were discussed a liability cap is provided. Moreover, in the only one in which there is no liability cap (the space liability convention) there is an absolute liability for the launching state and hence no liability whatsoever for private parties. However, in the literature with respect to these international conventions, these financial caps have been criticized. This criticism can be understood since financial caps (i.e. a general financial limits on the liability of industrial operators) adversely affect the realization of the goals and functions of tort law as they were summarized above.

Economic analysis supports the arguments against financial caps. From an economic perspective, it is important for the potential injurer to be fully exposed to the social costs of its activities to the extent these are within its control. Otherwise, the desirable internalisation of the negative externalities would not take place. In the literature, it has been argued that there may be good reasons to favour a strict liability rule for systemic risks, the main reason being that only a strict liability rule would lead to a full internalisation of the risks. This strict liability rule is especially recommended in a so-called unilateral accident situation, in which only one party influences the accident risk. Only with strict liability the potential injurer would also have an incentive to adopt an optimal activity level. This full internalisation is obviously only possible if the injurer is effectively exposed to the full costs of the activity it engages in and is therefore in principle required to provide full compensation to a victim. An obvious disadvantage of a system of financial caps is that this will impair the victim’s ability to obtain full compensation. But if the cap is set at a level much lower than the expected damage, this would violate not only the victim’s right to compensation, but also the principle of full internalisation of the externality. From an economic point of view, a limitation of compensation therefore poses a problem since there will be no internalisation of the full costs.

---

1036 Coase 1960, p. 1-44.  
1037 See above 5.5.1.  
1038 See 8.1.4.4.  
1039 Shavell 1980, p. 8 and 11.
As a closely related matter, given that the exposure to liability has a deterrent effect, a limitation of the amount of compensation due to victims poses another problem. There is a relationship between the magnitude of the accident risk and the amount spent on care by the potential wrongdoer. If liability is limited to a certain amount, the potential injurer will consider the accident as one with a magnitude of the limited amount. Hence, it will spend on care to avoid that an accident will be caused with a magnitude equal to the limited amount and it will not spend on the care necessary to reduce the total accident costs. In theory, the amount of care spent by the potential injurer will be lower and a problem of underdeterrence arises. The amount of optimal care, reflected in the optimal standard, being the care necessary to reduce the total accident costs efficiently, will be higher than the amount the potential injurer will spend to avoid an accident equal to the statutory limited amount. Thus, this theory predicts that as a result of the cap too little care is taken.\textsuperscript{1040} Despite suggestions by one stakeholder to the contrary, there is no reason to believe that the security industry is exempt from this economic mechanism.

Moreover, another effect of a financial limit on liability (in addition to providing undercompensation to victims and underdeterrence of operators) is that it would constitute an indirect subsidisation of the industry enjoying a particular limit on liability.\textsuperscript{1041} It should also be mentioned that in the areas where financial caps on liability exist, such as for marine oil pollution and nuclear liability, those limits are criticised in the literature on this ground.\textsuperscript{1042}

There is, however, one remarkable instrument that has been promulgated at EU level concerning auditors’ liability, the Commission Recommendation 2008/437, discussed in chapter 3.\textsuperscript{1043} The main advantage of this instrument is that it is merely a Recommendation and that it provides the Member States with various options for limiting liability, leaving the Member States to choose one of more of those options, or to refrain from taking any action. Those options were:

- establishment of a maximum financial amount or of a formula allowing for the calculation of such an amount;
- establishment of a set of principles by virtue of which a statutory auditor or an audit firm is not liable beyond its actual contribution to the loss suffered by a claimant and is accordingly not jointly and severally liable with other wrongdoers;
- provision allowing any company to be audited and the statutory auditor to determine a limitation of liability in an agreement.

We are not arguing at this stage that this is an ideal example that deserves implementation for the situation of the security industry, although we should note that a recommendation may be easier to justify than a legislative measure. However, if one were to decide upon a limit on the financial liability of the security industry, this approach has at least the major advantage of providing a lot of flexibility and leaving it largely up to the Member States to determine to the scope of liability, thus respecting the subsidiarity principle and having the benefits of flexibility and differentiation in light of Member States’ prevailing liability traditions.

\textsuperscript{1040} The reason for the underdeterrence is obviously the same as for the underdeterrence which results from the insolvency of the injurer. Underdeterrence arises because the injurer is not exposed to full liability, either as a result of his insolvency or as a result of a cap.

\textsuperscript{1041} See also Radetzki and Radetzki 2000.

\textsuperscript{1042} See for example as far as nuclear liability is concerned Trebilcock and Winter 1997.

\textsuperscript{1043} See supra 3.4.
Channeling of liability basically means that only one party can be held liable, thus excluding the liability of other parties involved.

Again, channeling of liability can be found in the liability regimes set forth in the international treaties described in chapter 5. As the comparative overview made clear, many of the international treaties channel the liability to a particular party, such as a ship owner (in the civil liability convention and the HNS convention) or the operator (in the nuclear liability conventions). As was explained in chapter 5, the current channeling of liability is beneficial to the security industry since it implies that it reduces the threat of liability from the security industry. However, the channeling is not perfect in all conventions. In some cases, the channeling is not exclusive and other parties can still be held liable. This is for example the case in the Montreal convention on international carriage by air.

Theoretically, one could envisage enlarging the channeling to an exclusive liability of operators (the customers of the security industry), thus preventing any liability of the security industry. However, also the channeling of liability has, more particularly with respect to nuclear liability and marine oil pollution been criticized in the literature. The main problem is that when liability is exclusively channeled to one liable operator this automatically excludes liability of all others who may also have contributed to the accident risk. If one believes that liability rules provide incentives for prevention, the disadvantage of channeling is that it removes the incentives for prevention from all parties other than the single operator to whom the liability is channelled.

The March 2011 Fukushima incident in Japan illustrates some of the undesirable consequences of channeling. The first reports on the Fukushima case made clear that the meltdown of the nuclear reactors may have been caused by the simple fact that the generators for the cooling system were located in the basement of the turbine buildings, which of course made them vulnerable to a tsunami. The question could be asked whether this is the result of negligent action by the operator TEPCO or rather the result of bad design or engineering by General Electric. In the latter case a channeling of the liability to the operator TEPCO would be problematic since channeling would lead to an exclusion of liability of all other parties who may have contributed to the risk, in this particular case (at least potentially) General Electric. The Fukushima case suggests that channeling can be problematic in removing incentives for prevention from other parties who are able to limit or otherwise influence a risk.

A similar argument could be formulated with respect to the liability of the security industry. In this respect it should also not be forgotten that the security industry is contracted by its clients precisely to provide the security they expect and that third parties (the public at large) also rely on the security industry to do what they are paid for, i.e. provide security. Fully excluding their liability by making customers exclusively liable from that perspective may also be undesirable.

---

1044 See supra 5.5.1.
1045 See 5.5.3.
8.2.4. Limiting causation

It is striking that neither in the European liability legislation, which was examined in chapter 3, nor in the international liability treaties examined in chapter 5, there are any specific rules dealing with causation. Causation may be a crucial issue since the security industry itself will normally never be considered a direct tortfeasor or injurer. The direct tortfeasor will normally be a criminal organisation or terrorist intentionally inflicting harm on victims. Moreover, a third party who intentionally acts to inflict harm will usually do it on the property of the customer (e.g. an airport) that contracted with the security company. The extent to which one accepts liability of the security industry is hence strongly related to the question whether one accepts that the behavior of the security industry has to be considered (if it is supposed wrongful) a cause of the damage suffered by the victim. Theoretically, it is possible to introduce strict requirements concerning causation and e.g. hold that in these particular cases damage could be recovered by victims only if their damage stands in a direct link with the fault or negligence of the security industry.

However, limiting causation would be a problematic policy option. So far, in all European legislation with respect to liability (discussed in chapter 3), there is no specific requirement for causation and those issues have always been left to the Member States. There are also good reasons for leaving causation issues to the courts. Causation is a complicated issue and deciding on issues such as the proximate cause or the remoteness of the damage is done differently in the Member States. Hence, it may be very difficult (if it would at all be politically desirable) to formulate a limitation on causation in such a way that it would be clear for all judges in the Member States which type of damage under which particular circumstances could still be attributed to the security industry. Hence, this would not appear to be a desirable route to take.

8.2.5. Relating liability to regulation

As we made clear at the end of chapter 3, many activities related to the security industry (although not necessarily the security industry itself in all aspects) are subject to detailed safety regulation. It was mentioned that safety regulation can have an important influence on liability. Compliance with regulation does not automatically exclude liability, but compliance could lead to a presumption of a security-related product not being defective. For example, compliance with the personal protective equipment directive may lead to an assumption of conformity with basic safety requirements, thus potentially reducing liability of operators.

The question arises what lessons could be drawn from this relationship with regulation for the security industry. On the one hand, the suggestion could be made to issue additional detailed regulations with which the security industry should comply. However, the comparative analysis also made clear that failure to comply with regulation is in all jurisdictions a strong indication that the defendant breached the required standard of care (common law) or acted unlawfully or negligently (civil law). Hence, it could be argued that the more regulation that is enacted, the more the liability of the security industry could potentially be expanded or limited. Indeed, as was argued in chapter 3, regulation in that sense constitutes a double edged sword: to the extent that the security industry complies with the regulatory standards, compliance could constitute a presumption of not having acted unlawfully (although that is not certain and debated), but non-compliance, on the other hand, will likely be regarded as

---

1048 More particularly in sections 3.6.3 and 3.6.4.
1049 See chapter 4 (section 4.3.2).
1050 Several countries already provide for special rules concerning the licensing of security companies and the supervision of their activities.
negligence per se. Compliance with safety regulation could generally increase care levels and thus reduce the accident risk and in that way limit the exposure to liability of the security industry. However, more detailed rules in safety regulation also make it easier for victims to prove that a particular regulatory standard has been breached, and, in that sense, the requirement of fault/negligence has been met. If the breach stands in a causal relationship with the damage of the victim, liability may be given.

Going a step further, one could argue that if detailed safety regulation were issued this would constitute more than just a presumption of lawfulness (which could be set aside if the court finds that the security provider nevertheless acted negligently). One could argue that compliance with safety standards, provided that those safety standards reflect optimal care levels, should exclude liability of the security provider. Although this position may obviously be quite desirable for the security industry (it would basically mean that as long as regulatory standards are complied with security providers are freed from a threat of liability), there are considerable problems with this option, both from a legal as well from an economic perspective.

From a legal perspective the problem would be that such a position would collide with the current principles of liability law and the tradition of the Member States. The mere fact that the operator complied with regulation is in most legal systems considered only a minimum and not a reason to exclude liability. That points at a second problem from a legal perspective: there is no legal system from those examined in chapter 4 that has a rule freeing an operator from liability if regulatory standards are complied with. Introducing such a rule would hence constitute a deviation from traditions in member state tort law.

There are also good economic reasons to reject a “regulatory compliance defence.” If compliance with a regulatory standard or licence would automatically result in a release from liability, the potential injurer would have no incentive to invest more in care than the regulation asks from it, even if additional care could still reduce the expected accident costs efficiently\[1051\]. A first reason to hold an injurer liable (if the other conditions for liability are met), although he has followed the regulatory standard, is that indeed this standard is often merely a minimum. A complete ‘regulatory compliance defence’ prevents any incentive to take precaution in excess of the regulated standard\[1052\]. Exposure to liability will give the potential injurer incentives to take all efficient precautions, even if this requires more than just following the regulation. This, by the way, holds both under negligence and strict liability. Since the regulatory standard can not always take into account all efficient precautionary measures an injurer can take, testing the measures taken by the injurer even though the regulatory standard was followed, will provide additional incentives. Allowing a regulatory compliance defence would also reduce the beneficial incentive effects of strict liability. Strict liability has the advantage that it provides the injurer with incentives to take all efficient measures to reduce the risk (prevention and activity level), even if regulatory requirements are followed. This outcome has been shown formally by Kolstad/Ulen/Johnson\[1053\] and by Burrows.\[1054\] They argue that a complete compliance defence prevents any precaution in excess of the regulated standard. If there is serious under-enforcement of standards, the role of liability as an incentive to take precautions remains important.

A second reason is that exposure to liability might be a good remedy for the unavoidable capturing and public choice effects that may play a role when regulations are adopted. If

---

1051 Shavell 1984, p. 365.
1052 Burrows 1999 p. 242. Later Schwartz added to the debate by discussing whether compliance with federal safety statutes should have a justificative effect in state tort cases; see Schwartz 2000.
1053 Kolstad, Ulen and Johnson 1990, p. 888-901.
1054 Burrows 1999, p. 227-244.
regulation would always release from liability, an operator would have strong incentives to
spend resources on securing a good regulation with easy conditions, because that would then
exclude any law suit for damages by a potential victim. Obviously, the capturing and public
choice effects could be addressed also via direct tools. In this respect, one can think of the
liability, even under criminal law, of regulatory authorities.\textsuperscript{1055} Liability of the regulatory
authorities (and appropriate sanctions within administrative law) can provide incentives to
civil servants to act efficiently when issuing regulations.\textsuperscript{1056} This, however, still requires tort
law to take into account the fact that regulatory standards are not always set efficiently. If the
optimal level of care is higher than the regulatory standard, liability will efficiently provide
additional incentives.

Finally, tort law can also be seen as a 'stopgap' for situations not dealt with by regulations.
This makes clear that the exposure to liability notwithstanding the regulations and/or permit is
an important guarantee that the plant operator will take efficient care.

8.3. Procedural solutions

If terrorist attacks or other large accidents result in widespread damage suffered by many
people, it is conceivable that many claims are filed against security industry providers in
several Member States. Consequently, security industry providers could be exposed to the
substantial costs associated with multiple cases pending in multiple jurisdictions. This raises
the question whether the EU should propose procedural solutions to reduce the burden
thereof.

In Work Package 1.5., we reviewed legislative instruments that are relevant to this issue. We
should note, however, that the EU has thus far not adopted any far-going requirements, for
instance, that all cases be centralized before one court. The problem of multiple claims
relating to one incident is not unique to the security industry, and may arise also in other
contexts where large scale damage occurs (e.g. an accident at a nuclear power plant, or a
defective product widely marketed throughout the EU).

We should note, too, that procedural solutions do not deal with any of the substantive law
issues, at least not directly. Some of these solutions, however, for example centralization of
all claims in one Member State court, do have implications for the applicable law, because the
laws of the Member States differ and these differences may have important consequences.

Procedural solutions could address the problem on an EU-wide basis (e.g. centralization in
one Member State), or at the level of each Member State separately. For instance, law suits
could be centralized for the whole EU, or they could be centralized within one and the same
Member State. Incidents giving rise to multiple claims in several Member States, of course,
are much rarer than incidents giving rise to multiple claims within the same Member State.

a. Litigation management, excluding the possibility of multiple simultaneous litigations

From a procedural viewpoint, in situations involving multiple cases, an important feature
could be centralization of all cases before one court. Multiple cases, of course, mean that
defendants have to respond to similar claims before multiple courts. This, in turn, means that
defendants incur multiple times similar costs, which inflates their aggregate cost, and each

\textsuperscript{1055} Faure, Koopmans and Oudijk 1996.

\textsuperscript{1056} Note, however, that industry may argue against such a liability of the authorities, as this may entail the risk that
authorities would be too reluctant in allowing emissions.
plaintiff incurs costs too. A rule that causes similar claims to be centralized before one court reduces the costs of defendants and plaintiffs.

Centralization could be a right of defendants. In that case, a defendant that is being sued before multiple courts could seek to have all claims against it transferred to one court. A defendant could do so, for instance, to reduce cost or ensure consistency of adjudication; multiple judgment, of course, creates a risk of inconsistency. It could also be a right of plaintiffs who could seek to centralize their claims to save on litigation cost. The latter is the concept of collective redress, a limited form of class action. Over the last couple of years, the Commission has studied the issue of collective redress. In June 2013, the Commission recommended collective redress mechanisms while ensuring appropriate procedural guarantees to avoid abusive US-style class action litigation. This recommendation does not cover centralization instigated by defendants, however.

As noted above, centralization could occur at the level of the whole EU, or at the level of each Member State. The Commission recommendation referenced above addresses the issue of collective redress at the level of each Member State, not at the level of the EU. Any regime for centralizing claims for the entire EU in one Member State needs to take into account the differences between the national law and procedure, as well as the difficulties associated with cross-border litigation. It is conceivable that any cost savings associated with EU-wide centralization will be substantially less than the cost savings result from centralization in each Member State separately. Centralization at the Member State levels also avoids the complexities associated with the differences between national laws, which may even mean that a person has a claim in one Member State but not in another Member State.

Any specific proposal to centralize claims against security industry providers should also justify why its scope is limited to the security industry. There would not appear to be a strong policy reason or objective justification for making this feature available only to security industry providers, and not to, for instance, airport operators, airlines, railway companies, etc. Indeed, any such centralization initiatives may have to be more general than merely the security industry.

b. EU-Member State in which incident occurs would be place of exclusive jurisdiction

One way to centralize claims is to grant the Member State in which the incident occurs exclusive jurisdiction. This would mean that all claimants would have to file their claims with the competent court of the Member State where the incident occurred. Conversely, they could not file with the courts of any other Member State. This would apply to any and all claims, including personal injury, property damage, pain and suffering, and pure economic loss.

There is some precedent within the current EU legislation. The Brussels I Regulation (Regulation 44/2001 on the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) seeks to eliminate obstacles deriving from incompatibilities between the various legal system and to facilitate access to justice based on the principle of mutual recognition and enforcement of judgements. It decreases the risk for the security industry to be sued in various countries for the same event of terrorism, since rules on tort and contractual claims as well as on *lis pendens* favour a single forum for the same event. However, because the state where the damage occurs may be hard to predict in the case of a terrorist act involving means of transportation (e.g., airplane), it is difficult for the security industry to determine in advance which law will apply. Likewise, the Service Regulation

---

(Regulation 1393/2007 on the service of judicial and extrajudicial documents) and the Evidence Regulation (Regulation 1206/2001 on cooperation in the taking of evidence) facilitate service of judicial and extrajudicial documents and the taking of evidence across Europe. These regulations may have a positive impact in the case of cross-border litigation involving terrorist cases and the security industry. In addition, the Rome I and II Regulations provide rules for determining the applicable laws.

The existing rules do not create a regime of exclusive jurisdiction of the courts of the Member State where the incident occurred. One policy option would be to establish such a regime, but the pros and cons, as discussed above, should be considered. Even though jurisdictional rules do not necessarily change the substantive rules governing the industry’s liability, in some cases, they would still deprive Member State courts of their current jurisdiction to hear claims.

c. Other exclusive jurisdiction options

Rather than granting exclusive jurisdictions to the Member States where the incident occurred, one could also give exclusive jurisdiction over claims to another Member State. The following options could, in theory, be considered:

- The courts of the Member State where the defendant resides. This option would centralize litigation against one and the same defendant, but not all claims relating to an incident. Another disadvantage would be that plaintiffs from other Member States would have to go to the defendant’s Member State.
- The courts of the Member State where the plaintiff resides. This option would not have much of a centralizing effect, but would allow plaintiffs to pursue claims before their own courts. As a toll for litigation management, it therefore has very limited effect.
- The courts of the Member State where the damage was suffered. In many cases, this would be the place where the plaintiff resides. Again, in cross-border cases, the centralizing effect may be limited.

As noted above, any of these procedural approaches should probably not be limited to the security industry, but apply to an objectively defined set of cases in which litigation management is complicated and results in substantial cost.

8.4. Human rights aspects of limitations on liability

8.4.1. Tort law and human rights

Since the Treaty of Lisbon the fundamental rights system of the EU is laid down by the Charter of Fundamental Rights of the European Union (CFR), which has the same legal value as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). Another important legal basis in this regard is provided by the fundamental rights of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of the European Council which, according to Article 6 TEU, constitute general principles of the Union’s law. Article 6 (2) TEU formally declares that the Union shall accede to the Convention.

---

1058 OJ 2012, C 326/391. The terms ‘fundamental rights’ and ‘human rights’ are used in this chapter as synonyms.
1059 Article 6 (1) TEU.
The obligations of the Charter are addressed to the institutions and bodies of the Union and cover all activities of these entities whether they are of a legislative or administrative character. The Member States are bound by the Charter insofar as they are implementing Union law both by legislation (e.g. implementation of directives) or administrative acts (Article 51 CFR).

The obligations to respect the rights and freedoms of the Charter are complex and comprise of two dimensions. The first dimension consists of the traditional function of fundamental rights to protect individual persons from unjustified infringements of their fundamental rights by the Union institutions respectively the Member States (negative obligation). As a second dimension, it is nowadays uncontested that fundamental rights also entail the positive obligation to ensure that the guarantees of the fundamental rights are implemented. Both obligations are expressed by Article 51 CFR which obliges institutions and Member States to ‘respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.’

That fundamental rights encompass positive obligations for the state is already recognised in the application and interpretation of the ECHR by the European Court of Human Rights. According to the jurisprudence of the court, the state must not only abstain from the infringement of fundamental rights of individuals, but must actively protect individuals against infringements by third parties. These duties may derive from all fundamental rights enshrined in the ECHR, but the European Court of Human Rights acknowledges that there is a broad discretion of the state as to the choice of means by which the state complies with this duty.

These principles also apply to the CFR.

When engaging in legislation the EU institutions must observe both the negative and the positive obligation deriving from human rights. This applies to all areas of legislation, hence also to the regulation of tort law and third party liability.

The CFR contains several fundamental rights that are relevant to tort law legislation. Article 2 (right to life) and Article 3 (right to the integrity of the person) relate to the protection of the integrity of the human body, Article 7 (respect for private and family life) to the protection of the development and the expression of the personality and Article 17 guarantees the right to property. These guarantees on the substance are complemented by the procedural guarantee of Article 47 CFR, the right to an effective remedy and to a fair trial.

All these rights are that are traditionally and prominently protected by the tort law system. The fact that they also constitute fundamental rights under the CFR (and also under the ECHR and the national human rights systems of the Member States) does not add much to the practical protection of these rights as they are already comprehensively protected by tort law. It, however, gives them a high degree of persistence and reduces the discretion of the legislature when dealing with them. This is reflected by Article 52 (1) CFR which requires that any limitations of fundamental rights must meet several conditions. First, they must be provided for by law; second, they must respect the essence of those rights; and third, they

1061 Jarass 2010, p. 428 et seq.
1063 Meyer-Ladewig 2011, p. 193; Grabenwarter and Pabel 2012, p. 131 et seq; Johann in Karpenstein/Mayer 2012, p. 39 et seq. See the decisions of the European Court of Human Rights in the cases Stubbings and others v the United Kingdom (Appl no 22083/93, 22095/93), Calvelli and Ciglio v Italy (Appl no 32967/96), Vo v France (no 53924/00).
1064 Jarass 2012, p. 432 et seq. See also Article 52 (3) CFR which provides that the meaning and scope of the rights contained in the Charter which correspond to rights guaranteed by the ECHR shall be the same as those laid down by the convention.
must comply with the principle of proportionality which requires that ‘limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’

When creating tort law provisions the legislature must consider these requirements, but, as is generally emphasised under the ECHR, the legislature has a broad margin of discretion. It may choose between different means to guarantee the protection of such rights, such as criminal protection, tort law liability, insurance mechanisms or even indemnification by the government. Moreover, when deciding on a rule, the legislature must consider that tort law rules regulate the legal relations between private persons and must therefore seek a balance between the interests of the injured person on the one hand and of the tortfeasor on the other.\textsuperscript{1066} While the legislature may not unduly restrict the right of compensation for the victim it must take care that the liability rules do not commit the tortfeasor to pay compensation sums that are completely out of proportion.\textsuperscript{1067} When dealing with tort law the legislature will foremost be obliged to consider the principle of proportionality, as expressly provided by Article 52 (1) CFR. It will thus be primarily prevented from the creation of rules which distinctly deviate from existing tort law rules without sufficient justification. From the ruling of the European Court of Human Rights in the case Budayeva and others v Russia\textsuperscript{1068} it may be deduced that the margin of appreciation is tighter with regard to the protection of human life than with regard to the protection of property.

Article 5 ECHR and Article 6 CFR further provide that everyone has the right to liberty and security of person (right to liberty and security). The right to liberty is, however, generally interpreted in the narrow sense as the right to physical liberty rather than physical safety, granting the individual person the right to move freely from one place to the other without undue interference by the state.\textsuperscript{1069} Article 5 ECHR thus does not, according to the jurisdiction of the ECtHR, oblige the state to grant the individual protection from bodily or mental harm.\textsuperscript{1070} Under the ECHR the right to security was traditionally regarded as being part of the right to liberty and was not attributed an independent scope of protection. This narrow interpretation extends also to Article 6 CFR.\textsuperscript{1071}

\textbf{8.4.2. Conclusions: The assessment of limitations on the liability of the security industry under human rights}

If the EU legislature chooses to create specific liability rules for the security industry, it will have to respect the rights and freedoms of the Charter of Fundamental Rights of the European Union (CFR) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Both systems oblige the legislature not to infringe the fundamental rights of individuals and to protect individuals against infringements by third parties. When deciding on the specific rules, the legislature has a broad margin of appreciation. It must respect the essence of the right to life (Article 2 CFR), the right to bodily integrity (Article 3 CFR), the right of the individual to private and family life (Article 7 CFR)

\begin{itemize}
  \item [1066] Berka 2011, p. 268.
  \item [1067] See European Court of Human Rights, Appl no 18139/91 Tolstoy Miloslavsky v the United Kingdom and the discussion of this decision by Berka, 2011, 280 et seq. Further cases are Steel and Morris v the United Kingdom (Appl no 68416/01) and Independent News and Media and Independent Newspapers Ireland Limited v Ireland (Appl no 55120/00).
  \item [1068] Appl no 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02.
  \item [1069] Hajduonová v Slovakia (Appl no 2660/03).
  \item [1070] Grabenwarter and Pabel 2012, p. 190.
  \item [1071] See Article 52 (3) CFR. See Jarass 2010, p. 73. For a broader interpretation Tettinger in Tettinger/Stein 2006 287 et seq who derives from Article 6 CFR the general obligation of the state to provide for the security of the citizens, albeit with a broad margin of discretion.
\end{itemize}
and the right to property (Article 17 CFR) and must comply with the principle of proportionality. It is the principle of proportionality that places the clearest demands on the legislature. In all Member States, tort law is a highly developed and sophisticated system. If the European legislator decides to modulate this system by issuing a rule that releases or protects the security industry from tort liability it can do so only if this interference is sufficiently justified.

8.5. Victim compensation solutions

We will now, relying on the analysis of legal practices with industries exposed to analogous risks (chapter 6), address a few other options that could be envisaged for providing adequate compensation to victims. From the outset, it should be stated that the policy objective then in fact becomes another one: the search is no longer for an instrument that would provide a limitation or protection to the security industry (as we examined above in 8.2), but rather a solution to provide adequate compensation to victims. In the situations we envisaged in this study, the security industry will usually not be a primary tortfeasor, but a secondary one; for instance, where a terrorist intentionally inflicts harm on an industrial estate where particular victims are present that suffer personal injury and other losses. As has been made clear, also in the comparative analysis victims would in that case most likely primarily call on the social security and social insurance providers. If particular losses were not compensated, the victim could either call on the liability of the facility where the incident took place (if, e.g., it were subject to strict liability as a guardian of a defective place) or of the security provider (again, assuming that the conditions for liability were met).

Addressing the question of victim compensation could in that sense be relevant for the security industry: if, for example, one were to create a victim compensation fund, or adopt another public fund solution, it would obviously decrease the risk that the victim would call on the security industry. A condition could be that the victim compensation fund would provide final payment to the victim and would not exercise recourse against the security industry.

This possibility is a relevant one especially since such a compensation fund exists in France for personal injury. For property damage in France compensation must be provided by the insurers. Also in many other European countries insurers, together with governments, have worked out specific facilities to deal with property damage created by terrorism. In that sense, as we have already discussed earlier, for terrorism-related property damage there is a solution in most European countries, which reduces the likelihood that victims will call on the security industry. One could hence examine whether also for personal injury a victim compensation fund of the type as it exist in France could be created at an EU-wide level. These options will now be reviewed.

8.5.1. Victim compensation fund

In the economic literature, often the question is asked to what extent a victim compensation fund can be considered more efficient in serving the goals of tort law than traditional insurance instruments. Applying the principles discussed above, there are not many reasons

---

1072 Chapter 4.
1073 Above we also made clear that this constitutes a substantial difference with the situation in the US, see supra 8.1.2.3.
1074 See supra chapter 4.
1075 These solutions have already been discussed in section 6.3.5.
why, if both are (in theory) available, a compensation fund would provide better protection against insolvency than the private insurance markets. One could assume that an insurer is better able to differentiate risks than a fund operator, since an insurer is specialized in risk differentiation and risk spreading. Insurers possess techniques to determine in what way their insured contribute to the risk. Obviously this assumes that the insurance markets are competitive. In the absence of competition in insurance markets, either the supply of insurance coverage could be too limited or premiums could be excessively high, which could justify a preference for a compensation fund. But if insurance markets are competitive, insurers can be assumed to be better able to deal with classic insurance problems such as moral hazard and adverse selection than the administrators of a compensation fund. This is so because it is hard to see why, as a matter of principle, a government agency that would run a compensation fund would have better information on risks than an insurer.

No matter how a compensation system is organized, the incentives for prevention of damage should remain adequate. Liability rules can have a preventive effect only if a duty to compensate is put on the one who actually contributed to the risk. This means that a duty to compensate should in principle only rest upon the one who actually contributed to the risk.

A second, related principle is that this duty to contribute should also be related to the amount in which the specific activity or entrepreneur contributed to the risk. This principle is usually automatically respected in liability law. The duty to compensate under tort law is indeed usually limited to the damage that the specific tortfeasor caused himself. However, also if a collectivization of the compensation takes place, it remains important to guarantee that the tort feasor only contributes financially in relation to the amount in which he contributed to the risk as well. This is reflected in insurance policies in the well-known idea of risk differentiation, which we have discussed previously. It simply means that bad risks pay a higher premium than good risks. This principle should also be applied if a compensation fund is established, meaning that bad risks should contribute more to the compensation system than good risks. This remains important since it will give incentives for prevention to the contributors to the fund. Bad risks will be punished and good risks should be rewarded.

These principles are not only important from an efficiency perspective (providing optimal incentives for prevention), but also from a fairness and justice perspective. Indeed, if these principles were not followed, it would mean that good risks would have to pay for, and thus subsidize, the bad risks. This negative redistribution should be avoided and therefore the compensation mechanism, fund or insurance, should be financed principally by the ones who actually contributed to the damage.

In sum, the compensation mechanism should aim at a differentiation of the contributions due. This differentiation is possible only if the insurance company or agency administering the fund also possesses information on the degree to which the specific activity contributed to the risk. One key element to determine the choice between insurance and funds is therefore who is in the best position to control the risk.

If both insurance and compensation funds are available, there are no reason why a fund would be the preferred solution; in fact, insurance offered in a competitive market is more efficient. As we have argued in chapter 6, first party solutions (like funds) may be desirable in case no liable injurer can be identified (like in the case of natural disasters). However, if a liable

1076 Faure and Van den Bergh, pp. 65-85.
1077 Unless there is joint and several liability or channelling of liability.
1078 See supra 6.4.6.
injurer can be identified (either the customer/operator or the security provider) creating a fund would be undesirable, since it would typically exclude the liability of the liable tort feasor.

The crucial question would be how any compensation fund would be financed. In accordance with the principles we just sketched, a fund should be financed by those who create the risk (operators and/or the security industry) and, moreover, the contributions should be risk-related. In that sense, the French fund for compensation of victims of terrorism is problematic since it is not financed by operators or other potentially liable injurers, but via a tax on property insurance contracts. Hence, in France, the potential victims themselves finance the fund and not operators. This seems to collide with principles of prevention and correct risk allocation as discussed above.\(^{1079}\) In the French model of a compensation fund, not operators but rather those who have property insurance contracts pay for the fund and hence for the compensation of potential victims. For the reasons we discussed, this solution does not deserve copying at the European level.

### 8.5.2. Government provided compensation

#### 8.5.2.1. Arguments in favour

Although there are obvious (economic) criticisms that can be formulated of government-provided compensation, there are some positive aspects as well. A positive aspect of government intervention is that the prospects of large-scale payments in the aftermath of a security industry-related disaster might encourage the government to take cost-benefit justified precautions long before disasters strike.\(^{1080}\) This argument could be made in the case of damage resulting from a security industry-related disaster. A large terrorist attack can lead to a total disruption of society. Providing ex post relief may then help to restore public trust. Moreover, governments may be better able to determine adaptation strategies necessary to react against the disaster, at least when compared to potential victims. Think of the example of large infrastructural works which would be necessary to prevent damage resulting from security industry risks (if it were already possible e.g. to ex ante invest in prevention). These are typically the public goods that would not be provided through private action and may hence require government intervention.

A related argument in favour of government intervention would be that government has the capacity to diversify the risks over the entire population and to spread past losses to future generations, thus creating a form of cross-time diversification, which the market could not achieve. The argument could be made that in some situations the government is in a better position to adapt to disasters than individuals\(^ {1081}\) or even to prevent certain security-related risks. Government intervention from this perspective would provide incentives to politicians to invest in preventive measures.

Moreover, one could also make the argument that government can (in principle) compensate without predefined limits. If the damage would exceed the current budgetary possibilities of the government, as mentioned above, cross diversification over time and future generations could in principle take place.

\(^{1079}\) See supra 8.1.4.4.

\(^{1080}\) See Levmore and Logue 2003, p. 310.

\(^{1081}\) This argument has been strongly made in relationship to terrorism by Kunreuther and Michel-Kerjan 2004.
8.5.2.2. Arguments against

Notwithstanding those theoretical possibilities of government compensation, the arguments against such compensation are compelling as well. The most convincing argument is a very simple one and is precisely the same argument advanced in the literature related to the international conventions on nuclear liability against government compensation (via the second and third layer). If government *de facto* provides compensation to victims, it effectively provides a subsidy to industry as a result of which industry will be able to externalize the social costs of its activity. The negative consequences of such subsidies are well-known:

- It is no longer the one who causes the accident and creates the risk who has the burden of compensation, but society at large and ultimately the tax payer, which is an undesirable distributional consequence;
- Since operators are not confronted with the total costs related to their activity, their level of prevention will be too low and their activity level will be too high. Liability rules, if government takes part of the compensation for its account, cannot have their desirable deterrent effect. Increased accident risks and lower levels of safety can be the result;
- As a consequence, operators will invest less in safety measures (not being confronted with the total costs of their activity) and will not bear the total damage that could result from their activities. The consequence will be that relative prices are too low which can be considered a market failure. In that hypothetical case, relative prices of oil and gas (especially compared to e.g. renewable energy) would be relatively low, since prices would not reflect full social costs. Again, from a social welfare perspective that would be an undesirable result.

Further, where the government outsources security to the private sector, this can be regarded as the government’s determination that private parties are in a better position to prevent the risks at issue. This confirms that the private security providers, not the government, should be responsible if such risks materialize.

8.5.2.3. Policy recommendation

On the basis of this reasoning, it is clear that direct compensation by government is not a preferred option to deal with security industry-related damage. That is not to say that there should be no role whatsoever for government in the aftermath of a disaster caused by a security industry-related incident. Relief measures and coordinating disaster management in the immediate aftermath of the disaster are undoubtedly tasks where the government can play an important role. However, a critical condition would be that if steps are taken, either in restoration (e.g. of destroyed infrastructure) or providing immediate relief to victims, the price for those interventions are ultimately allocated to the liable operator (either via the liability system or otherwise). This corresponds to sound economic principles of costs internalization and to the polluter-pays-principle.

It should also be stressed that none of the stakeholders we interviewed suggested that a (partial) compensation by government would be a desirable option to deal with the compensation of security industry-related damage; their focus has been on third party liability limitation, as is demonstrated, for instance, by the ASSA International/CoESS position paper entitled “A European Solution for Third Party Liability of the Aviation Security Services Providers,” which calls for “appropriate solutions that limit liabilities incurred by all commercial parties,” and the ASD/EOS position paper entitled “European Union Third Party Liability Limitation,” which calls for a “binding liability cap valid in any European court of justice.”
8.5.3. Government providing an additional risk layer

In chapter 6, we suggested that if there, in fact, are demonstrated to be supply side problems with insurance, public-private partnerships could be developed whereby government would provide additional capacity and would act as reinsurer of last resort. Of course, it would be important that government does so in the least distortive way possible and, for example, only intervenes by stimulating market solutions and charging a risk-based premium (thus avoiding subsidisation and promoting a market solution). As we discussed in chapter 6, those types of solutions have been specifically worked out with respect to terrorism-related risks. Therefore, capacity has been created which will precisely reduce the likelihood that victims will have to call on the liability of the security industry.

8.5.4. Mandatory financial security

One potential issue not discussed yet is whether one should consider the introduction of mandatory financial security to be provided by the security industry to cover its potential liability exposure. Several arguments or criteria in favor of compulsory financial security are examined below.

One argument is related to information problems. Information problems might arise in case the potential injurer cannot make an accurate assessment of the risk it is exposed to and/or the benefits of the purchase of insurance. An underestimation of the risk would in that case lead to the wrongful decision of the injurer not to purchase liability insurance. The legislature could remedy this information problem by introducing a general duty to insure. This information problem is probably a valid argument to introduce a general duty to insure for motor vehicle owners. Maybe the average driver of a car underestimates the benefits of insurance. If there would be no information problem and the legislature would nevertheless introduce a duty to insure, because this would be "in the best interest" of the insured, this would reflect mere paternalism.

If empirical evidence would exist that the security industry would greatly underestimate the costs of damage it may cause, and the probability that they will be held liable for this damage, this would then lead injurers to reserve too few resources to cover their potential liability. If these conditions are met and one can indeed assume that injurers underestimate the cost of damage, this information deficiency may be considered an argument in favour of compulsory insurance. But again, the policy argument based on information asymmetry relates merely to the fact that the injurer would underestimate the potential benefits of insurance. However, this argument does not seem very convincing in the case of the security industry where there is no proof of specific information deficiencies. The industry appears to be well aware of its exposure, and suggests that insurance is either unavailable or priced at levels that make it prohibitive. This is also a possible problem; if few security companies seek insurance, it is harder for insurance providers to develop attractive products, because of problems relating to potential adverse selection and the lack of the benefits of the law of large numbers.

Another argument for introducing compulsory financial security would be the potential insolvency of an injurer. Insolvency may, however, pose a problem of under-deterrence. If the expected damage exceeds the injurer's assets, the injurer will only have incentives to purchase insurance up to the amount of its own assets. It is indeed only exposed to the risk of losing its

1082 See Bruggeman, Faure and Heldt 2012, p. 221-223.
1083 See section 6.3.5.
1084 This was also the opinion of representatives of a large reinsurer, interview on 12 March 2013.
own assets in a liability suit. The judgement proof problem may therefore lead to underinsurance and thus to under deterrence. Jost has rightly pointed at the fact that in these circumstances of insolvency, compulsory insurance might provide an optimal outcome. By introducing a duty to purchase insurance coverage for the amount of the expected loss better results will be obtained than with insolvency whereby the magnitude of the loss exceeds the injurer's assets. In the latter case, the injurer will indeed only consider the risk as one where it could at most lose his own assets and will set his standard of care accordingly. When it is, under a duty to insure, exposed to full liability, the insurer will obviously have incentives to control the behaviour of the insured. Via the traditional instruments for the control of moral hazard, the insurer can make sure that the injurer will take the necessary care to avoid an accident with the real magnitude of the loss. Thus, Jost and Skogh argue that compulsory insurance, provided that the moral hazard problem can be cured adequately, can provide better results than under the judgment-proof problem. This is one of the explanations why, for instance, for traffic liability compulsory insurance was introduced. Uninsured and insolvent drivers who have little money at stake which they may lose compared to the possible magnitude of accidents they may cause, may have little incentives to avoid an accident. Insurers might better be able to control this risk and could force the injurer to take care under the threat of shutting him out of the insurance. Thus, the insurer becomes a regulator of the insured activity.

Indeed, this economic argument shows that insolvency may cause injurers to externalise harm: they may be engaged in activities that may cause harm greatly exceeding their assets. Without financial provisions these costs would fall on society and would hence be externalised instead of internalised. Such an internalisation can be achieved if the insurer is able to control the behaviour of the insured. The insurer could set appropriate policy conditions and an adequate premium. This suggests that if the moral hazard problem can be cured adequately insurance leads to higher deterrence than a situation without liability insurance and insolvency.

However, also this argument is not particularly convincing either in the case of the security industry. Throughout this study, we have argued that as of yet (and probably in the future as well) the exposure of the security industry to liability risks is not of such a nature that this would be uninsurable and that large insolvency risks are likely to emerge if companies are not negligent. Moreover, if one were to consider the introduction of mandatory financial security, the more logical step to take would be to impose mandatory financial security on operators, the clients of the security industry. As we have shown in chapter 5 dealing with the international treaties related to nuclear safety, civil aviation and environmental liability, many of those treaties do indeed impose compulsory financial security. Hence, since we also have argued that it is more likely that liability will be focussed on the operators who may be victims of particular security breaches (e.g. by terrorists) it is also logical that a duty to obtain financial security is imposed upon those operators rather than on the security industry.

Since there is also no convincing evidence yet that there are huge insolvency risks as a result of which the security industry may not be able to meet its liabilities towards third parties,

---


1086 See also Kunreuther and Freeman 2001, p. 316.

1087 See the overview in section 5.5.1 above.
imposing mandatory financial security upon the security industry would hence potentially only create huge administrative costs without compensating benefits.

8.6. Prerequisites in institutional European law

In theory, options to address the security industry’s liability exposure range from a Safety Act-like regime to a non-binding Commission recommendation on the application of existing civil liability rules to security industry providers, to no action at all. As discussed in section 7.4.2, the Safety Act is specific to the US with its complicated and rich civil liability system. The liability exposure of security companies is a function of this system, and this exposure necessitated the Safety Act. The European liability landscape and litigation environment, as discussed in section 8.1.2.1 above, is different, and these differences substantially reduce the necessity of a Safety Act-like regime. Even if it were deemed justified to prevent potential problems in the future, these differences would affect the design of any such regime.

In this section, we expand the analysis presented in section 7.4.2, and review perquisites in European law for possible options to address the liability of the security industry. While a full-fledged Safety act regime requires an institutional framework at EU level, other options raise more limited issues under EU law. The two main issues arise in relation to the EU’s powers to legislate (‘competence’) and general principles of EU law.

8.6.1. EU Competence

The EU does not have explicit authority to legislate in the area of national security, nor does it have explicit power to enact civil liability law. As Article 5 of the TEU provides, the limits of EU’s competences are governed by the principle of conferral, i.e. the EU has power only where such power is explicitly bestowed on it.\footnote{Article 5(2) TEU provides: “Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.”}\footnote{This corresponds to Task 6.3 of the Invitation to Tender.}

The Treaty on the Functioning of the EU (TFEU) defines three types of legislative powers (‘competences’) of the EU, as follows:

- **Exclusive competences under Article 3 of the TFEU**: These powers do not appear to be directly relevant to any possible TPL measures.

- **Shared competences under Article 4 of the TFEU**: Both the EU and the Member States are authorized to legislate in these areas, but the Member States may exercise their power only where the EU has not legislated. Article 4(2) lists as shared competences the “internal market” and “freedom, security and justice.” Under Article 26 of the TFEU, the EU has the power to adopt “measures with the aim of establishing or ensuring the functioning of the internal market,” which comprises “an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.”

- **Supporting competences under Article 6 of the TFEU**: The EU has the power to legislate only to support, coordinate or complement the Member States’ policies. Consequently, it has no legislative power in these fields and may not interfere in the exercise of these competences reserved for Member States. These areas include health protection, industry, and civil protection.
In addition, the EU has special competences in some areas (such as the coordination of economic and employment policies pursuant to Article 5 of the TFEU), but these are not directly relevant to TPL legislation. Further, pursuant to the “flexibility clause” set forth in Article 352 of the TFEU, the EU can be authorized to act if necessary, but unanimity in the Council is required.

Under Article 4(2) TEU, national security remains the sole responsibility of each Member State. Further, Article 346 TFEU (ex Article 296 TEC), under (b), provides that ‘any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes.’ Pursuant to Article 73 TFEU, ‘it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.’ Although not directly relevant to the issue of allocation of powers, Article 6 of the Charter provides that ‘everyone has the right to liberty and security of person.’

Thus, national security policy is not a power of the EU. It should be noted, however, that legislation on third party liability (TPL) of the security industry is probably not national security policy. Like other policies and laws, such legislation may indirectly influence national security policy, but is likely not part thereof.

The EU does not have explicit powers to legislate on civil liability, but liability legislation may be covered by another EU competence. This raises the question what the legal basis could be for EU legislation on TPL of security providers. A plausible legal basis for such legislative measures could be the EU’s internal market powers. The internal market title of the TFEU gives the EU broad authority to adopt measures ‘with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties.’

To this end, the ‘internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.’ As discussed in Chapter 4, the issue of the security industry’s third party liability plays out somewhat differently in different Member States. To some degree, the nature and magnitude of the liability exposure varies based on the national law of the Member States. Differences in liability exposure could result in different competitive conditions and in barriers to trade in goods and services between the Member States. For instance, a security provider from a Member State where the liability exposure is low, may be reluctant to sell products in a Member State where the liability exposure is high. This may be so, for instance, where a security provider does not have adequate insurance in place, because such insurance is not needed in his home country. Thus, differences in third party liability exposure of security providers may affect the movement of goods, persons, and capital between the Member States. If differences in TPL between the Member States indeed affect the free movement of goods and services and frustrate the objective of establishing an internal market (which this study has not analyzed), the EU has the power to take measures to address any such differences.

Thus, the conclusion is that the EU, based on its internal market powers, has the power to adopt TPL legislation for the security industry, including legislation along the lines of the US Safety Act, subject to compliance with the Treaty and general principles. In particular, if any

1090 Article 26 TFEU (ex Article 14 TEC).
legislation is based on the EU’s internal market powers, the requirements for the exercise of the internal market powers must be met.

8.6.2. General Principles of EU Law

In legislating, the EU must respect the relevant provisions of the Treaty and general principles of EU law.\(^\text{1091}\) For example, EU legislation should meet the subsidiarity and proportionality principles set forth in the TFEU. As Article 5 puts it, ‘[t]he use of Union competences is governed by the principles of subsidiarity and proportionality.’ Any EU TPL legislation, of course, would have to comply with these principles. Under the principle of subsidiarity, as Article 5(3) of the TEU provides, in areas which do not fall within its exclusive competence, the EU “shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.” This principle could be met if there is a problem in the internal market for security goods and services and such problem cannot be adequately addressed through only national measures. TPL legislation could be justified on this ground.

Under the principle of proportionality, as Article 5(4) of the TEU provides, the content and form of EU action “shall not exceed what is necessary to achieve the objectives of the Treaties. In theory, TPL legislation could meet this requirement (note, however, that this study has found any evidence of actual problems in relation to the security industry’s liability exposure). The analysis, however, should be done on a case-by-case basis in light of a specific measure and specific facts. Obviously, a fledged Safety Act regime is more likely to raise issues in relation to proportionality than a Commission recommendation.

Likewise, EU measures should be consistent with other principles of EU law, such as the equality principle, and legal certainty and legitimate expectations.\(^\text{1092}\) With respect to the latter, we can be brief: there is no generic reason why TPL legislation would raise issues of legal certainty and legitimate expectations. Of course, in a specific case, such issues may arise, but that is not inherent to TPL legislation as such. The equality principle, on the other hand, is directly relevant to any possible TPL legislation. As TPL legislation, by definition, provides some sort of liability limitation to a specific liability regime for the security industry, the question arises why the security industry should be singled out: why shouldn’t all companies benefit from this program, or at least all companies that are exposed to potential catastrophic, large scale damage? Under this principle, an objective justification is required for the differential treatment of the security industry.\(^\text{1093}\) Thus, the EU will have to provide an adequate objective justification to avoid a risk that TPL measures might be challenged successfully.

8.7. Summary and evaluation

In this concluding section, we summarize and evaluate the various policy options open to the Commission based on the findings of this study. We point out where issues arise, what plausible policy responses may be available, and what implications and consequences various policy options will have. In assessing the situation, we take the arguments of the security

---

\(^{1091}\) Tridimas 2006.

\(^{1092}\) Craig 2012.

industry as a starting point and discuss those in light of the findings of this study. We then summarize our key findings, the possible policy responses, and their consequences.

8.7.1. Analysis of arguments for TPL limitation in favour of the security industry

Stakeholders have argued that the security industry is different from other industries in relation to third party liability exposure for terrorism-related damages. They believe that security providers are exposed to unlimited “enterprise-threatening” liability vis-à-vis third parties, due to the unavailability of insurance and their customers’ refusal to grant contractual liability limitations. Based on this study, as discussed below, the argument that security providers are exposed to unlimited third party liability has to be seriously qualified, and the claims about insurance and contracting problems, even if supporting empirical evidence were available (which stakeholders have not provided), cannot justify a general liability limitation for all security providers.

The argument that terrorists and other aggressors are intentionally and actively using their best efforts to “beat” security products and services, does not mean that the security industry is liable if they succeed. The merits of this argument depend on the nature and scope of industry’s liability exposure for terrorism (see further below).

Further, the argument to the effect that security products providers cannot disclose the limits of their products and services, is right, but, again, the issue is whether this is held against them under civil liability law. Likewise, other arguments that could be made (‘the customers of the security industry, not the security providers themselves, decide which goods and services are procured,’ and ‘terrorists are generally attacking a state or fighting the government, not the security product provider’) may also be right as a matter of fact, but even if they are, the question arises whether and, if so, to what extent, the security industry is exposed to liability as a result of these facts. The argument presented above relating to immunity, as well as the argument to the effect that the security industry is told by regulators what security to provide, should also be analyzed in light of the actual liability exposure of the security industry. Once that analysis is done, a different picture arises.

In Chapter 4, the results of the national law analysis were presented. This analysis provides a picture of the actual liability exposure of security provides under the national laws that we studied. From this analysis, we may conclude that the security industry’s liability exposure is not nearly as expansive and “enterprise-threatening” as some industry representatives assume. We have reached the following conclusions:

- Security providers are not exposed to strict liability. If terrorists are able to beat security measures, the security industry is not liable based on that fact by itself. More than merely damage and some causal link with the security activity is required.

- Security providers are liable on the basis of negligence based on the standard applying to security professionals. Under product liability law, their liability vis-à-vis third parties is primarily for manufacturing defects; design and warning defects are assessed in light of the agreement with the customer. Thus, the fact that the security provider is unable to disclose the limits of security technology to the public does not result in liability exposure. In any event, exposure under European product liability law is limited to personal injury and property damage.

- National liability laws recognize that security providers are not making the critical decisions about what equipment and services to use at facilities. A security provider is not liable on the grounds that not the best equipment and services were deployed. This implies too that a security provider is not liable merely because terrorists were
able to beat the system. The fact that binding rules may regulate the security industry (or its goods or services) may mean that the security provider can invoke a ‘mandatory order’ defense.

- Thus, the fact that terrorists attack the state, not the security provider, does not mean that the security provider should therefore be immune from law suits. National law, however, takes due account of the security provider’s contractual obligations and does not impose an independent standard of care in relation to third parties. Thus, the standard of care that the security provider has contractually agreed is also the standard in third party law suits.

- Under national law, the security industry is not, or hardly, exposed to liability for economic damage (lost profits), and punitive or treble damages do not exist. Thus, the security industry’s exposure is limited primarily to personal injury and property damage (and the latter primarily in the context of recourse by insurers against them).

- Under national law, security providers can exclude by contract liability for terrorism-related damage. If they do so, they are exposed only to negligence liability for non-terrorist risk. Security providers can limit their primary obligations (e.g., they can stipulate that they do not address terrorism risk) and negotiate liability limitations (such as financial limits, or the exclusion of certain types of damage). Exoneration with respect to personal injury, however, is generally not possible (note, however, that a reinsurer mentioned that personal injury is not a main problem with respect to insurability; the main problem is property damage). There is asserted to be a problem, however, in that the customers of the security industry are unwilling to agree reasonable liability limitations (the study team did not receive nor find any evidence of such problems, however).

Security industry providers thus do not appear to be exposed to excessive or even significant liability risks under the national laws of the Member States studied. The exposure of a security provider is chiefly a function of two factors: (1) whether it was negligent, and (2) what the contract with its customer provides. Both of these factors are, in theory, within the control of security providers, and, therefore, a liability limitation is very hard to justify as a policy choice, because it may well reduce incentives to prevent damage across the board and raises the issue of who will compensate damages falling outside the security providers’ scope of liability.

8.7.2. Summary of key findings, possible policy responses, and their consequences

Based on the findings of this study, we see little evidence of an impending liability crisis in the security industry. There have been no cases in which security providers have been held liable for damages caused by terrorist attacks. We are not aware of security providers being unable to provide goods or services due to excessive liability exposure, and have not seen any evidence suggesting as much. Potential liability under national law for terrorism-related damage requires negligence, and is limited in terms of heads of damages to which liability attaches, and contractual liability limitations are generally enforceable. This is good news, also for the security industry itself.

It may be regarded as surprising that security industry representatives have argued for years in favor of liability limitations without ever having conducted any analysis of the industry’s actual liability exposure in Europe. We believe that this could possibly be explained by two factors. First, these stakeholders may have simply extrapolated from the liability situation in the US, without recognizing that the EU litigation environment is very different. Second, based on the experience with the process leading to the adoption of the US Safety Act, they
may have believed that any such analysis would or should not be expected of them. Nevertheless, the continued strong but unsubstantiated claims about the industry’s “enterprise-threatening” liability exposure, remain difficult to understand in the European context. As discussed below, to alleviate the confusion, the Commission might therefore want to consider initiatives aimed at informing the industry about the nature and extent of its liability exposure.

We do not want to suggest, however, that there is no problem at all. As noted above, like all other operators, security providers may be exposed to liability where they are negligent, or where they breach their contractual obligation. Under the national laws of the Member States, liability based on negligence is generally financially unlimited; note, however, that any such liability requires breach of a duty of care or fault, and applies not only to security providers but to all legal and natural persons. Security providers have also complained about the lack of affordable insurance and the reluctance of their customers to agree reasonable liability limitations, which are allegedly issues that would indirectly affect the industry’s third party liability exposure.

Policy options involving liability limitations and related instruments can be analyzed with respect to contents (substance) and form. In relation to substance, policy responses can be grouped into six main categories:

1. A full fledged Safety Act-like regime;
2. Other liability limitations, notably, a liability cap, exclusion of certain types of damage from the scope of liability, or a regulatory compliance exception;
3. Initiatives addressing issues in the markets for security goods and services;
4. Initiatives aimed at the insurance market;
5. Measures aimed at creating alternative compensation mechanisms; and
6. Initiatives aimed at informing the security industry, and, as necessary, insurers, Member States, and other stakeholders about issues relating to liability, insurance, and contracting.

In addition, there is, of course, the option to do nothing.

With respect to the form, for our purposes, three groups of EU measures can be distinguished:

1. Legislation (directive or regulation) to implement one or more of the possible policy options;
2. Non-binding policy measures, such as recommendations and communications; and
3. Other initiatives that are aimed at obtaining and disseminating sound and reliable information relevant to third party liability exposure of the security industry, insurance, and contracting.

Each of these main substantive categories and forms is briefly discussed below.

- Safety Act

A Safety Act, of course, would be in the form of binding legislation. For the reasons discussed, we do not see a need for a EU Safety Act. The EU liability environment is very different from the US liability environment, and the reasons that necessitated the US Safety Act are not present in the EU. Any proposed EU Safety Act would have to meet the proportionality principle and the principle of equality, which is not self-evident.

If the EU decides to pursue a Safety Act, a EU level agency would have to be designated to deal with the certification and designation of security products and services. Some features of the US Safety Act, such as the prohibition of punitive damages and litigation solely before
federal courts, simply do not apply in Europe. The costs of operating an EU Safety Act regime will be substantial, while the benefits will be less clear.

In light of the findings of this study, we believe that a Safety Act would be an exaggerated policy response to what appears to be a limited problem.

- Other liability limitations

In addition to an EU Safety Act, other limitations of the liability of security providers could be enacted. Possible options include a liability cap (i.e. a financial limit or ceiling), the exclusion of certain types of damage from the scope of liability (e.g. pure economic loss), or a regulatory compliance exception (e.g. if a product or service meets all applicable regulatory requirements).

These options have different pros and cons, but a common issue is the effect on incentives to prevent damage. If the EU decides to pursue a liability limitation, it should consider, and mitigate, as necessary, the effect on prevention incentives. If a financial cap is set at an appropriately high level (e.g. up to insurance limits), little effect on incentives is to be expected; the lower the limit, the stronger the adverse effect on incentives may be, but this is also a function of regulatory and contractual standards. The exclusion of pure economic loss is also an option, but national laws are already quite reluctant to extend liability to include such losses in any event. A regulatory compliance exception or defense is an option that should be tied to a good program of regulatory standard-setting and updating; if no guarantees exist for adequate and comprehensive standard-setting and updating, a regulatory compliance exception may not be a good idea.

If any liability limitation is deemed appropriate, it could be issued in the form of a non-binding policy measure. For instance, the EU might consider a recommendation an appropriate instrument to address liability limitations. There is precedent at the EU level for such a recommendation in the form of Recommendation 2008/437 on auditor’s liability. A communication would be an alternative. We will discuss this option further below. Note, however, that this study has not found evidence of problems that should be addressed through a liability limitation.

- Initiatives addressing issues in the market for security goods and services

This study did not involve an independent analysis of the functioning of the market for security goods and services. However, security industry representatives have suggested that a problem exists because many purchasers are public or quasi-public bodies that contract for security goods and services through open public procurement procedures. As a result, there is little or no room to negotiate reasonable liability limitations and indemnities. We have found that in the software industry liability limitations are common practice, and apparently do not result in problems of under-deterrence.

If indeed there is a problem of market failure in the markets for security goods and services (for instance, concerted action by public authorities to disallow liability limitations and indemnities), the EU could play a role in facilitating more flexible procurement processes. Such EU action could involve open discussions between security authorities, operators of airports and the like, and the security industry to discuss issues and identify and agree best practices. Once the nature and scope of the problems is understood, a Commission recommendation on contracting for security goods and services is also a possible option. Binding legislation, however, is not an option that can likely effectively and efficiently address this issue.
As this study found no evidence of any such issues, however, the Commission could consider, as a preliminary step, to call on the security industry to provide documentary evidence of the issues and produce a sound analysis. In the absence of any such facts and analysis, there would appear to be no basis for decision making by the Commission.

- **Initiatives aimed at the insurance market**

Security providers complain about the unavailability and unaffordability of insurance, in particular against the risks of terrorism. A large reinsurer, however, has informed us that it is not aware of such problems. Information provided by Insurance Europe, on the other hand, suggests that the situation may differ significantly between EU Member States. This suggests that further analysis of the insurance market may be useful to get better insights into the nature of any issues that arise.

In addition, the EU could play a role in facilitating discussions between the insurance industry and the security industry. Such discussions could also be helpful in understanding and resolving any problems. Again, if there are issues in the insurance market, a Commission recommendation might be a suitable instrument to address these issues.

It should be noted, however, that the security industry stakeholders have merely asserted that there are insurance problems, without providing any substantiation. As a first step, therefore, these stakeholders could be asked to produce documentary evidence of the nature and scope of the problems in each of the EU Member States. Once this evidence has been analyzed, informed decisions can be made.

- **Measures aimed at creating alternative compensation mechanisms**

As discussed before, compensation funds and similar measures to take the burden of liability off the security industry do not appear to be indicated at this point. In general, such measures will have adverse effects on incentives to prevent damage and raise a host of other issues (who will fund, on what basis, rights of recourse, etc.). Limited alternative compensation mechanisms covering, for instance, pure economic loss or for losses in excess of any liability cap, could be considered, however, if a need were to arise.

In any event, before the EU should even consider any such measures, it should explore other available policy options; if such options are not feasible, alternative compensation mechanisms might be considered. In designing any alternative compensation mechanisms, the EU should ensure that efficient prevention of damage remains a goal. Note, however, that this study has not found any significant need for such measures.

- **Initiatives aimed at informing the security industry and, as necessary, insurers, Member States and other stakeholders about issues of liability (and, if necessary, insurance and contracting)**

This study has shown that key stakeholders are confused about security providers’ potential liability exposure in EU Member States. Civil liability has not been harmonized at EU level to any significant extent, and understanding the liability laws of 28 Member States can be a daunting task. Thus, the Commission might consider initiatives aimed at disseminating accurate information about security providers’ liability exposure under EU and national laws. Such initiatives could include information sessions, case studies, workshops, websites, and the like.

Likewise, it is conceivable that Member State governments and judges, insurers, and other stakeholders may have a need for reliable information about liability, and any insurance and contracting issues. Again, the Commission could play a facilitating role here and promote the
dissemination and exchange of accurate information, for example, about the situation in other Member States and ‘best practices.’

- A Commission recommendation or communication?

Although this study found no evidence of actual problems, a Commission recommendation or communication could be considered to prevent potential problems from arising in the future if and when a large-scale terrorist attack were to occur. Future problems cannot be entirely excluded because liability laws work with ‘open’ standards (such as fault or negligence) that allow for potentially expansive interpretation and application. Note, however, that this issue extends beyond security providers to other sectors of industry that are exposed to liability for identical or similar ‘catastrophic’ risks.

Any Commission action would likely be most effective once any issues surrounding insurance and public procurement have been documented and analyzed. We should emphasize also that this study analyzed the liability laws of only 7 out of 28 Member States. To complete the picture and avoid issues of unjustified extrapolation or generalization, an analysis of the laws of the other Member States would be useful.

Any such recommendation or communication could cover the following aspects:

- Explain the potential for an expansive interpretation and application of liability laws to cause problems for security providers in the case of large scale damage arising from terrorist attacks.
- Set out various principles by which such liability can be kept within reasonable limits in future cases. These principles could include the following:
  - National liability laws recognize that security providers are not making the critical decisions about what equipment and services to use at facilities. A security provider is not liable on the grounds that not the best equipment and services were deployed.
  - Security providers are not exposed to strict liability; a security firm is liable if it is at fault, acts negligently, or provides a product that suffers from a manufacturing defect.
  - The standard of liability applying to security providers is not the standard applying to lay persons, but a higher standard that is appropriate for security professionals. This standard is not so high, however, that only the best security firms can meet it; it is the expertise and skill of a reasonably experienced and skilled security provider that is required.
  - Liability law takes due account of the security provider’s contractual obligations and does not impose an independent standard of care in relation to third parties. If a security provider is held liable by a third party for terrorism-related damage, the agreement between the security provider and the facility operator defines that scope of the security provider’s obligations, including its obligations to accept liability. Liability limitations set forth in that agreement, in principle, also have effect vis-à-vis third parties, except, possibly, with respect to personal injury.
  - Any alleged design defects are assessed in light of the agreement with the customer-operator.
  - The fact that the security provider is unable to disclose the limits of security technology to the public does not result in liability exposure for failure to warn.
  - The fact that binding rules may regulate the security industry (or its goods or services) may mean that the security provider can invoke a ‘mandatory order’ defense, or benefit from a rebuttable assumption of having met the required due care standard.
Liability for property damage and consequential and pure economic loss can be mitigated in light of all relevant facts, including insurance (both first and third party). Punitive or treble damages are not appropriate in civil liability.

- Address any issues in the insurance market. Of course, the specifics can be set out only once these issues have been documented and analyzed.
- Address any issues in the market for public procurement of security goods and services. Likewise, the specifics can be set out only once these issues have been documented and analyzed.

8.7.3. Final conclusions

This study has not found any evidence of an impending liability crisis in the security industry. The assertions of ‘enterprise-threatening’ liability exposure are not consistent with the liability standards under the laws of the 7 Member States covered in this study. No urgent EU measures are therefore necessary. To prevent problems in future cases, a Commission recommendation or communication could be considered. Possible elements of such an instrument have been discussed in the preceding section. Given the confusion and fear among security industry stakeholders, it may be helpful to launch initiatives aimed at enlightening the security industry and, as necessary, insurers, Member States, and other stakeholders about third party liability exposure.

Security industry representatives have also claimed that there are problems in the insurance market and in the market for public procurement of security goods and services. Although these issues do not justify a liability limitation, they may deserve further attention from policy makers, either at the EU or Member State levels. The industry could therefore be invited to provide further evidence and analysis of any such issues.
List of References

**American Law Institute 1991**

**Ameye 2010**

**Ammerlaan and Van Boom 2003**

**Association of European Airlines 2013**

**Batsch 1998**

**Bergkamp 2003**

**Berka 2011**

**Bidan 2001**

**Bier 2006**

**Bigus 2008**

**Bishop 1983**
Blanchard 2000

Bocken 2006

Bruggeman 2011

Bruggeman, Faure and Fiore 2010

Bruggeman, Faure and Haritz 2011

Bruggeman, Faure and Heldt 2012

Burgherr and Hirschberg 2008

Burrows 1999

Cabantous 2007

Calabresi 1970

Cane 1999

CCR 2007

Chao 1996
Coase 1960

Congressional Research Service 2007 (US)

Craig 2012

Croley and Hanson 1995

CSES 2012

CSES 2012
CSES, Interim Evaluation: impact of the REACH Regulation on the innovativeness of the EU chemical industry (European Commission), June 2012.

Currie 2008

Daniels, Kettl et al. 2006

De Smedt 2009

De Smedt and Faure 2010

Dobbs 1986

Doherty et al. 2008
Doherty, N.A. et al., Managing Large-scale Risks in a New Era of Catastrophes, Wharton Risk Management and Decision Processes Center in conjunction with the Georgia State University and the Insurance Information Institute, 2008.

Dute, Faure and Koziol 2004a
Dute, Faure and Koziol 2004b

ECORYS 2012

Emons 2001

Endres, Ohl et al. 2003

Epstein 1985

Epstein 1995

Epstein 1996a

Epstein 1996b

Erhard-Cassegrain 2004

Ernst & Young 2013

European Commission 2008

European Commission 2009
European Commission 2010

European Network and Information Security Agency (ENISA) 2011

Faure 1993

Faure 1995

Faure 1998

Faure 2000

Faure 2001

Faure 2002

Faure 2003

Faure 2004a

Faure 2004b

Faure 2006

Faure 2007
Faure 2010a

Faure 2010b

Faure 2010c

Faure 2011

Faure and Betlem 2008

Faure and Bruggeman 2008

Faure and Fenn 1999

Faure and Fiore 2009

Faure and Grimeaud 2003

Faure and Hartlief 1995

Faure and Hartlief 1996
Faure and Hartlief 1998

Faure and Hartlief 2001

Faure and Hartlief 2002

Faure and Hartlief 2003

Faure and Hartlief 2006

Faure and Heine 2000

Faure and Heine 2005

Faure and Heine 2002

Faure and Hu 2006

Faure and Koziol 2001a

Faure and Koziol 2001b

Faure and Liu 2012a

Faure and Liu 2012b
Faure and Philipsen 2008

Faure and Van den Bergh 1995

Faure and Vanden Borre 2008

Faure and Wang 2006

Faure and Wang 2008

Faure, De Roos and Visser 2001

Faure, Fernhout and Philipsen 2009

Faure, Fernhout and Philipsen 2010

Faure, Koopmans and Oudijk 1996

Faure, Lixin and Hongjun 2010

Faure, Peeters, Philipsen and De Smedt 2010

FBE Management Ltd 2012
FBE Ltd., TSI and CSA, Guidance Note on the Construction Products Regulation - Version 1 April 2012
Fondazione Rosselli 2004

Freeman and Kunreuther 1997

Frey and Stutzer 2002

Frey and Stutzer 2004

GAO 2003

GAO 2005

Gilead 1997

Gluver and Olsen 1998

Gollier 2005

Grabenwarter and Pabel 2012

Gron and Sykes 2002

Gron and Sykes 2003

Hall 2011
Harrington 2000

Hartington et al. 1997

Hartlief 2003

Hartwig 2002

Hinteregger and Kissich 2004

Hockman, Lowe et al. 2004

Hodges 1993

Holoubek 1997


Huber 1991

Huber and Amodu 2006

Hunter and Bergkamp 2001

Jametti and von Ungern-Sternberg 2004
Jametti and von Ungern-Sternberg 2006

Jarass 2010

Kakalika and Pace 1986

Kaplow and Shavell 2001

Kapenstein and Mayer 2012

Koch 2010

Kolstad, Ulen and Johnson 1990

Koziol 1997

Krämer 2005

Kunreuther 1968

Kunreuther 1993

Kunreuther et al. 1995

Kunreuther 1996
Kunreuther 2008

Kunreuther and Freeman 2001

Kunreuther, Hogarth and Meszaros 1993

Kunreuther and Michel-Kerjan 2004

Kunreuther and Michel-Kerjan 2005

Kunreuther and Pauly 2005

Kunreuther and Pauly 2006

Lafay, Cannarsa and Moréteau 2006

Lamm 2006

Langbein 1995

Levmore 2003

London Economics 2006
Magnus 2006

Magnus 2010

Magnus and Mankowski 2007

Mandel 1999

Marshall 1974

Martí Sempere 2010

Martí Sempere 2011

Mason 2003

Medaglia et al. 1995

Meurkens and Nordin 2012

Meyer-Ladewig 2011

Michel-Kerjann 2010

Miller 1982
Millington 1987

Monti 2001

Moréteau, Cannarsa et al. 2006

MPI 2007

OECD 2005a

OECD 2005b

Pelzer 1982

Pelzer 1988

Pelzer 2007

Perry 2004

Philipsen 2009

Philipsen 2012

Polinsky and Shavell 2010
Priest 1985

Priest 1987

Priest 1989

Priest 1991

Priest 1992

Rabin and Bratis 2006

Ramseayer 2011

Rauch 1995

Richardson 2000

Riegel, Miller and Williams Jr. 1976

Russell and Thomas 2008

Sands and Peel 2012
Schwartz 1983

Schwarz 2000

Schwartz 2009

Schwartz and Wilde 1979

Schwarze and Wagner 2004

Shavell 1980

Shavell 1984

Shavell 1986

Shavell 1987

Shavell 2000

Shavell 2007

Shughart 2006

Slovic, Fischhoff et al. 1977
Slovic, Fischhoff et al. 2000

Slovic, Kunreuther and White 2000

Smets 1983

Smithies 2007

Snijders 1993

Sobel and Leeson 2006

Spier 1998

Spier and Haazen 1998

Steins Bisschop and Olaerts 2010

Stiglitz 1983

Szczekalla 2002

Tanega 1996

Toffoli et al 2005
Trebilcock 1987

Trebilcock and Daniels 2006

Trebilcock and Winter 1997

Tridimas 2006

Tunc 1996

Vallet 2005

Van Dam 1993

Vanden Borre 1999

Vanden Borre 2001

Vanden Borre 2007

Vanden Borre 2010
Van Schoubroeck 2002

Van Velthoven 2009

Vásquez-Maignan 2012

Verheij 2007

Verkerk 2009

Verkerk 2010

Viscusi 2010

Viscusi and Zeckhauser 2012

Von Bar 1996

Von Ungern-Sternberg 1996

Von Ungern-Sternberg 2007

Wagner 2005
Walter and Kettl 2006

Weitzdörfer 2011

Wang 2007

Wang and Faure 2010

Watabe 2006

Wendel 2004

Wenneras 2005a

Wenneras 2005b

Wood 1975

Yamori and Okada 2007

Zeckhauser 1996
Annex I: Common format for analysis

Common Format for Analysis of Liability and Regulatory Regimes

In analysing laws and regulations covered by the Study, we use a specific format for ease of reference and to increase comparability between regimes. This format is very similar to the tentative checklist presented in our Proposal. We first present the format for the analysis of liability regimes and then for the regulatory programs covered by this study. If a law includes both a regulatory and liability regimes, each will be analysed separately on the basis of the formats specified below.

In addition to a brief analysis of the liability or regulatory regime concerned, the analysis focuses on (1) whether and, if so, how the regime affects the liability exposure of security services providers; and (2) whether any concepts or features of the regime could be usefully applied in defining a potential liability regime for the security industry. As appropriate, applications or examples are provided. These aspects are addressed whenever in the analysis they appear relevant and in a concluding section at the end.

Liability regimes

In the case of liability regimes, the following issues are covered in the order as listed:

1. Brief summary of the regime
In a few paragraphs, the essence of the regime is summarized. This brief summary is intended to give the reader a quick overview of the regime so as to enable him to put the more detailed analysis that follows into context.

2. Basis of liability
Is liability based on fault (negligence), strict (no-fault) liability, or another standard? No-fault liability is potentially broader than liability based on negligence, although this depends also on the fault standard and other features such as exclusions and defences and the rules of evidence (see below). The standard can also be defined in terms that do not resemble the strict/fault liability dichotomy (e.g. a defect in a product).

3. Liable persons (attribution of liability)
Who is exposed to liability under the regime? Is liability channelled to only one party? Does the doctrine of joint and several liability potentially apply? Is there a right of contribution or recourse against any other person?

4. Damage covered
A liability regime does not necessarily establish liability for all possible damages that may result from a covered activity. We discuss whether the following types of damage are covered:
   a. property damage;
   b. personal injury, including medical expenses and loss of income;
   c. pain and suffering (also called “moral” damages); and
   d. economic damage (also called “lost profits”).
In addition, we verify whether liability is subject to any qualitative or quantitative monetary limits (also called “financial caps”).
5. Exclusions and defences
Are any persons, activities or products excluded, completely or partially, from the liability regime? Is there an exemption for a defence industry provider, or a government contractor? Any such exclusions are analysed and described.
Further, does a defendant have defences available to it? If so, which defences are available and how do they work? Does the concept of force majeure encompass acts of terrorism?

6. Causation
Does the law specify a rule regarding causation, i.e. the causal link between the putative damage-causing event and the damage for which compensation is sought? What are the criteria for determining causation? How does the law deal with causal uncertainty?

7. Relation with regulation
How does the liability regime relate to any applicable regulatory regimes? In theory, regulation could expand potential liability exposure, and/or limit potential liability exposure. Liability could be expanded because (i) the regulation increases the applicable standard, (ii) the regulation requires disclosure of information on the basis of which claims can be asserted, (iii) non-compliance with the regulatory standards constitutes breach of obligation or negligence per se, which may trigger liability exposure, and/or (iv) other regulatory requirements tend to increase liability exposure. Liability could be limited because (i) the regulation relaxes the applicable standard, (ii) the regulation requires disclosure of information on the basis of which the defendant can assert a defence or argument defying liability, (iii) compliance with the regulatory standards constitutes a preclusion or defense, also called the regulatory compliance defence, and/or (iv) other regulatory requirements tend to limit liability exposure.

8. Financial security and compensation mechanisms
Does the regime (or practice pursuant to the regime) provide for any special financial security or compensation mechanism (in addition to or in lieu of the standard procedure under civil procedure)? Such provisions could involve (a) insurance, (b) mutual or pooling schemes, or (c) other financial security instruments, such as bonds, bank guarantees, or cash deposits? A related question is whether any compensation obtained through social security schemes, or other insurance or compensation mechanisms?

9. Rules of evidence
Does the regime set forth special rules of evidence? Who bears the burden of proof? Are there any presumptions of a causal link? If so, under which conditions do they apply? Can the burden of proof be shifted to the defendant?

10. Jurisdictional and procedural issues
These issues are addressed only in relation to EU liability regimes. Key questions are (i) which courts have jurisdiction to hear claims under the regime (courts of the plaintiff’s home country, and courts of the defendant’s home country), (ii) whether multiple claims can be managed to increase efficiency (e.g. centralize claims in one court, or suspend proceedings until one claim has been resolved, etc.), (iii) whether there are specific rules regarding cross-border claims or compensation, (iv) how the applicable law is determined, and (v) how judgment obtained in one Member State can be recognized and enforced in another in another Member State.

11. Conclusion and Relevance to the Security Industry
This section will set forth the conclusions and consider how relevant the regime and any of its constituents elements are to the security industry’s actual or potential liability exposure, and any potential liability limitations.
Regulatory regimes

The analysis of the regulatory regimes proceeds along different lines. The following issues are covered in the order as listed:

1. Brief summary of the regime
   In a few paragraphs, the essence of the regime is summarized. This brief summary is intended to give the reader a quick overview of the regime so as to enable him to put the more detailed analysis that follows into context.

2. Key Objectives
   What are the objectives of the regulation?

3. Key Instruments
   Which instruments does the regulation employ to achieve the objectives? Possible instruments include (i) informational, reporting, and disclosure requirements vis-à-vis government agencies and/or consumers, (ii) production or design requirements (means and/or results requirements), including European standards, (iii) registration, notification, or authorization requirements, and (iv) post-marketing monitoring requirements and related reporting obligations, and (v) warning or recall obligations if issues are discovered post-marketing.

4. Regulated entities and activities or products
   What persons are subject to the regime? What activities and products are regulated?

5. Relation with liability
   Does the regime specify any rule in relation to civil liability? Even if it does not do so, in theory, regulation could expand potential liability exposure, and/or limit potential liability exposure.
   Regulation could expand liability exposure because (i) it increases the applicable standard, (ii) it requires disclosure of information on the basis of which claims can be asserted, (iii) non-compliance with the regulatory standards constitutes breach of obligation or negligence per se, which may trigger liability exposure, and/or (iv) its requirements tend to increase liability exposure in some other way.
   Regulation could limit liability exposure because (i) it relaxes the applicable standard, (ii) it requires disclosure of information on the basis of which the defendant can assert a defence or argument defying liability, (iii) compliance with the regulatory standards constitutes a preclusion or defense, also called the regulatory compliance defense, and/or (iv) other requirements tend to limit liability exposure.

6. Financial security and compensation mechanisms
   Does the regime (or practice pursuant to the regime) provide for any special financial security or compensation mechanism? Such provisions could involve (a) insurance, (b) mutual or pooling schemes, or (c) other financial security instruments, such as bonds, bank guarantees, or cash deposits?

7. Transition
   Does the regime provide for rules relating to transition and/or grandfathering? If so, how do these rules work?

8. Conclusion and Relevance to the Security Industry
   This section will set forth the conclusions and consider how relevant the regime and any of its constituents elements are to the security industry’s actual or potential liability exposure, and any potential liability limitations.
Annex II: Overview of stakeholder participants

On 20.11.2012 separate interviews were held in Brussels with the following groups of stakeholders:

- Confederation of European Security Services (COESS) and Securitas (two respondents)
- European Organisation for Security (EOS), Boeing, Smiths, Safran for GIFAS (in total five respondents)
- Euralarm (three respondents)

In presence of:
- Michael Faure (METRO)
- Lucas Bergkamp (Hunton & Williams)
- Nicolas Herbatschek (Hunton & Williams)
- Anke van Bergeijk (Hunton & Williams)

On 06.12/2012 an interview was held in Brussels with a representative of ACI Europe

In presence of:
- Lucas Bergkamp (Hunton & Williams)
- Nicolas Herbatschek (Hunton & Williams)
- Anke van Bergeijk (Hunton & Williams)

Written questionnaire responses or other information were received from respondent(s) of the following organizations:

- American Chamber of Commerce to the EU
- Boeing
- Euralarm
- European Organisation for Security (EOS)
- GIFAS
- a European insurance association
- a reinsurer

The following organizations were represented at the stakeholders meeting on 12 September 2013 in Brussels:

Airport Council International (ACI) Europe
American Chamber of Commerce to the EU
ASSA International (ASSA-I)
Boeing
Confederation of European Security Services (COESS)
ECTIL
Euralarm
European Commission, DG ENTR
European Organisation for Security (EOS)
Finmeccanica
GIFAS
Hunton & Williams
Insurance Europe
Kramer Levin Naftalis & Frankel LLP
Lloyd’s
Maastricht University, METRO
Munich Reinsurance Company
Securitas
Siemens AG
Smiths Detection / Smiths Group
Thales
Universiteit Antwerpen
TPL Security Industry Project Questionnaire

Email:

Dear [name of stakeholder representative]:

The University of Maastricht, Hunton and Williams, and ECTIL have been awarded a Commission contract for a study on third party liability of the security industry. The team will have its first meeting on November 2.

We understand from the Commission that your association has expressed concerns about the liability exposure of security goods and/or services providers. In preparation for our meeting, it would be useful for us to review any information you may have relating to this topic, including legal analysis, legal opinions, studies on the effects of perceived liability risks, case law, etc. Would you be so kind at to send us any such materials prior to November 1?

Further, we would like to meet with you in person in Brussels. Would you be available on November 20?

Please do not hesitate to contact us if you have any questions.

Sincerely,

Michael Faure
Lucas Bergkamp

Questionnaire:

This questionnaire is intended for use with the security industry (SI). The questions are intended to guide the discussion with SI representatives, but are not exhaustive and other issues may arise.

If a question is answered affirmatively, further details are typically necessary to fully understand the issue. Where any relevant written documents are available, we would appreciate receiving copies.

I. Civil Liability in Europe

A. Liability concerns

1. Could you please explain why liability has become a major concern for the SI?

2. What has changed in (i) law, (ii) society, or (iii) otherwise for liability to have become a major concern now? Is the actual or perceived increased risk of terrorism the main driver?

B. Liability claims and judgments

3. Have claims been asserted against SI providers by (i) third parties or (ii) contracting parties with respect to damage for which they were held responsible?
4. If so, what have been the basis and size of any such claims?

5. Have there been court judgments against SI providers?

C. Liability insurance and other risk-spreading arrangements

6. Are SI providers insured against liability risks? If so, what are the relevant terms and conditions, exclusions, and limits of such insurance?

7. Have SI providers been denied insurance coverage?

8. Have SI providers entered into other risk-spreading arrangements such as mutuals or risk pools?

D. Effects of potential liability on innovation and economic activity

9. What have been the effects of the threat of liability on the SI? What has been the effect on innovation?

10. Have any been technologies, products or services not been made available, or been made available, due to the threat of liability?

11. Have any empirical studies been conducted on these issues?

II. US Safety Act

12. Has the US Safety Act had any competitive effect on EU-based SI providers?

13. Have EU SI providers been able to benefit from the liability protection offered by the US Safety Act? If not, why not?

14. Does the protection offered by the US Safety Act help US SI providers operating on the EU market? If so, how?

15. Does the European SI industry feel that a regime like the US Safety Act is necessary and justified? If so, why?

III. Solutions

A. Structuring and Contractual solutions

16. Do SI providers use the ‘corporate shield’ (i.e. limited liability entities) to protect against liability? If not, why not? If so, how does it work and what has been the experience?

17. Do SI providers use contractual mechanisms such as exoneration, indemnities, and limitations such as financial limits, to limit their liability exposure? If so, why are these insufficient? If not, why not?

B. Legislative solutions

18. Does the SI feel that the legislature should intervene to address the issue of liability for security products and services? If so, how is the exposure of the SI different from the
exposure of other industries (e.g., accounting, credit rating agencies, software companies, biotechnology companies, etc.)?

19. What is the preferred solution the legislature should adopt? Why? Should this solution apply only to the SI? Should the EU adopt it, rather than the Member States?

20. Is there anything else we should know?