ECORYS

Study on Civil Military Synergies in the field of Security

Final Report

Client: European Commission DG Enterprise & Industry

Rotterdam, May 2012

Study on Civil Military Synergies in the field of Security

Final Report

Client: European Commission DG Enterprise & Industry

Rotterdam, May 2012

ECORYS

About Ecorys

At Ecorys we aim to deliver real benefit to society through the work we do. We offer research, consultancy and project management, specialising in economic, social and spatial development. Focusing on complex market, policy and management issues we provide our clients in the public, private and not-for-profit sectors worldwide with a unique perspective and high-value solutions. Ecorys' remarkable history spans more than 80 years. Our expertise covers economy and competitiveness; regions, cities and real estate; energy and water; transport and mobility; social policy, education, health and governance. We value our independence, integrity and partnerships. Our staff are dedicated experts from academia and consultancy, who share best practices both within our company and with our partners internationally.

Ecorys Netherlands has an active CSR policy and is ISO14001 certified (the international standard for environmental management systems). Our sustainability goals translate into our company policy and practical measures for people, planet and profit, such as using a 100% green electricity tariff, purchasing carbon offsets for all our flights, incentivising staff to use public transport and printing on FSC or PEFC certified paper. Our actions have reduced our carbon footprint by an estimated 80% since 2007.

ECORYS Nederland BV
Watermanweg 44
3067 GG Rotterdam

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com
Registration no. 24316726

W www.ecorys.nl

Table of contents

1 Executive Summary

1.1 Introduction

This Executive Summary describes the findings from the "Study on Civil-Military Synergies in the field of Security", which is one of the studies undertaken in the context of the Framework Contract on Security (ENTR/09/050) between the European Commission, DG Enterprise and a consortium led by Ecorys Nederland B.V. The main tasks of this study were:

- To map the most successful areas of spin-offs in the last decade.
- To identify technological areas with the highest potential of synergies between the civil security and military sectors.
- To identify the economic models used by industry to identify areas of interest for civil-military spin-offs.
- To conduct an impact assessment of policy options, proposed by the Commission, and
- To suggest further policy options and measures that might help to strengthen synergies between the civil security and military sectors.

1.2 Background

The key security threats to Europe have changed dramatically over the last two decades. While the risk of large-scale aggression against any member of the European Union (EU) has become very low, other threats such as terrorism, proliferation of weapons of mass destruction, state failure and cybercrime have gained in relative importance. Traditionally, security risks were divided into external risks, i.e. originating outside the territory of the state, and internal or domestic risks. The former were the domain of military, the latter of civil (non-military) security forces. However, many new types of security threats do not fall neatly into one of these categories. Indeed, the European Security Strategy emphasizes that "none of the new threats is purely military nor can any of such threats be tackled by purely military means alone"[1]. Instead, it calls for a mix of instruments and close cooperation between the military and the security domains.

These developments clearly indicate that the dividing lines between defence and security are becoming much less clear cut than before.[2] Responding to the new security threats often requires close cooperation between defence and security forces, which indicates (or might indicate for the future the possibility of) some blurring between their missions as well. This dynamics presumably has significant implications for the capability requirements of the forces and services involved and, therefore, for defence and security industries.

Despite the fact that 'security' stands high on the political and societal agenda, until recently the security sector has not received much attention from the competitiveness and industrial policy perspective. The EU security industrial base is quite weak and the internal security market is highly fragmented with widely different national regulatory frameworks[3].

---

1 "A Secure Europe in a Better World. European Security Strategy", Brussels, December 12, 2003.

2 Istituto Affari Internazionali, IRIS and Manchester Institute for Innovation Research, "Study on the industrial implications in Europe of the blurring of dividing lines between security and defence", 2010, study commissioned by the European Commission.

3 EC "An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage", COM(2010) 614

Within this context, one option to strengthen the security industrial base is to (further) enhance cooperation between the civil security and military industries and promote technological spin-offs between them. This might help reduce unnecessary duplications and to expand the market for defence and security companies that are able to successfully capitalise on civil security-military synergies. Indeed there have been numerous calls by the European Council to promote synergies between security and defence technologies.[4]

Another factor that makes this policy option important is the on-going and expected reductions in public expenditure in most EU countries. Many European countries will have to implement significant fiscal adjustments to stabilize and reduce their public debt. Stricter budget constraints suggest that public expenditure on procurement of civil security and military equipment might be smaller in the near- and medium-term future. Promoting spin-offs between the civil security and defence industries could help to save public money and contribute to the rationalization of these industries.

The pressure on defence budgets after the end of the Cold War was a major incentive for military to move to a more extensive use of commercial technologies and equipment in the defence systems (the other main reason was technological leadership of the commercial sector in several key technological fields, such as information technologies). The use of commercial off-the-shelf (COTS) products in the military field can be seen as a general case of the spin-offs from the civilian (commercial) sector to the defence sector. Advantages and disadvantages of the greater use of COTS items in military have been extensively discussed in the literature.[5]

Civil security and defence markets

The defence sector in Europe, commonly referred to as the European Defence Technological and Industrial Base (EDTIB) can be demarcated relatively easily, even if it consists of sub-sectors that have very different industrial, technological and market characteristics and different military requirements.[6] The demand side is clearly defined: the end-users of military products and services are almost entirely made up by national Ministries of Defence (MoDs). This concentration on the demand side is to a large extent reflected on the supply side as well. Lead systems integrators, platform producers and producers of weapon systems are mainly large companies, primarily "national champions", specialized on defence production. These so-called 'prime' contractors subcontract specialised systems producers, for example in electronics, and producers of complete sub-systems or major components. Often, these 'tier 1' contractors are also risk sharing partners. Although only few of these prime and tier 1 companies produce exclusively for the defence market, they are very much aware of their status as defence companies and are fully organized to the particular characteristics of the military market. The clear and focused structure on both the demand and the supply side leads to the well regulated and close interaction between the two sides. Established, long term relationships are important. This situation constitutes a significant barrier for new entrants to the defence market.

From a technological point of view, the defence sector is characterized by a long term and integrated approach, often caught under the term "capability based planning". The various MoDs across Europe set clear military requirements for the longer term. Military equipment typically has a

4 http://www.ess-project.eu/news/83-the-european-council-insists-on-development-of-civil-military-synergies.html

5 See, for example, Defence Science Board, "Buying Commercial: Gaining the Cost/Schedule Benefits for Defence Systems", February 2009.

6 TNO, "Development of a European Defence Technological and Industrial Base", 2009, study commissioned by DG Enterprise & Industry.

life of several decades. In many cases, the defence industry is involved in defining the technical specifications for equipment that are derived from these requirements. The demand side is prepared to share risks in technology and platform development. Although the influx of 'civil' technology has increased over the past decades and will continue to do so, the defence technological base is still quite clearly defined. Again, this forms a barrier for new markets entrants, in particular innovative SMEs.

Defence total expenditure in the EU reported by the EDA (for 26 participating Member States, excluding Denmark) amounted to €194 billion in 2009. This includes approximately €41 billion spent on equipment procurement and R&D.[7] Three countries with the largest defence budgets – France, the UK and Germany – together account for approximately two thirds of all defence investment (equipment procurement and R&D) in the EU. Globally, the United States is by far the largest defence market, representing approximately 75% of NATO-wide defence equipment expenditures. Military R&D expenditure in Europe amounted to €8.56 billion in 2010. Around 90% of this amount was spent by three countries: France, UK and Germany.[8]

The trade body for European defence firms – the AeroSpace and Defence Industries Association of Europe (ASD) – estimates total turnover of the European aerospace and defence industries as €162.9 billion in 2010. These companies directly employed 704 thousand workers. [9]

In marked contrast to a firmly established defence sector, the scope and perimeters of the security sector are highly amorphous. The concept of a civil 'comprehensive security' domain has only taken shape over the last decade or so. This conceptual idea of a (more or less) cohesive domain spanning elements of security that in the past were largely disconnected, is only partially reflected in the real world. Despite some national initiatives to develop a more structural and long term approach, the demand side remains very fragmented. Its core typically consists of the Ministry of the Interior, that typically has lead responsibility for national security, and of various auxiliary services and security agencies. Increasingly other ministries, regional and local government as well as public and private operators of infrastructure also have a stake in comprehensive security (whole-of-government approach); as do citizens and societal organisations (whole-of-society approach, societal resilience). Many of these stakeholders are not used to formulate their needs in terms of functional requirements and capabilities over a longer period of time, let alone consolidate these in a joint vision and strategy. The fragmentation on the demand side is mirrored on the supply side, which is neither well defined nor clearly identifiable in terms of recognised classifications of industrial activities.[10] Unsurprisingly, the sector lacks clearly defined and shared technology roadmaps which, in turn, impedes structural and substantial technology investments.

Furthermore, the security technological base is not very distinctive. Many technologies in the security field are applicable across different sectors (for example, protective clothing, mobile communication, IT and network security, etc). As a result, many security sectors to a large extent overlap with the safety and other civilian industries, which often leads to widely different definitions of the security industry and its size. R&D expenditure in the security industry is significantly smaller than in the defence industry, notably because of a stronger focus on cost containment, the lack of

---

7 http://www.eda.europa.eu/Libraries/Documents/National_Data_Breakdown_Publication_pMS_1.sflb.ashx.

8 EDA Defense data portal.

9 ASD, Facts and Figures 2010.

10 ECORYS, DECISION and TNO, "Study on the Competitiveness of the EU security industry", 15 November 2009, study commissioned by DG Enterprise & Industry

'mass' on both the demand and the supply side, as well as a lack of longer term (shared) visions as the driver for technology roadmaps.

The general size of the security market depends on its definition, with estimates ranging from €49.2 bn to €103 bn. The larger figure takes into account "physical security protection", which is not counted in some definitions, and includes the use of CCTV, access control equipment, intrusion and detection systems, and protective clothing.

Summing up, the defence and civil markets have significant differences:.

- on the demand side: consolidated and public for defence, fragmented and public and private for civil security;
- on the supply side: clearly demarcated for defence, blurred for civil security;
- on the interaction between demand and supply: well structured and centralized for defence, decentralized and locally structured in security;
- and with respect to technology and product development: longer term technology roadmaps and cost and risk sharing drive innovation for defence, little dedicated innovation for security.

Definitions and Framework

To ensure consistency and common understanding, especially in the area where multiple terms with a similar meaning are widely used, it is important to be clear and precise with terminology at the outset. The title of the project refers to civil-military synergies in the field of security. In a general sense, a synergy can be defined as "the interaction of two or more organisations [..] or other agents to produce a combined effect greater than the sum of their separate effects".[11] In the present context a civil-military synergy implies a greater effectiveness or efficiency, achieved through combined actions or cooperation between the civil security and the military sectors than would or could be achieved separately.

Synergy is a broad term and the study focused on a particular form of synergy – technological spin-offs between the civil security and military sectors (in both directions) which we understand as the application of a technology developed primarily for one sector in the other sector.

When discussing "technology" it is helpful to distinguish three different technology levels:[12]

1. Integrated platforms and systems;
2. Equipment and sub-systems;
3. Technologies and components.

These three technology levels have different innovation dynamics, as well as differences in the demand side and supply side. This leads to differences in the potential for synergies.

- "Technologies" are essentially "neutral", in the sense that technologies are not inherently military or civilian, their applications are specific. Thus, they often have application across a wide variety of civil, security and military areas. Critically, where technologies originate (whether it is the defence or civil industry) influences the ways and possibilities of their diffusion and use;
- For (integrated) "systems/platforms" the potential for synergies tends to be most difficult to bring to fruition. The design and specification of systems/platforms emerge from a close relationship between the supply side (companies) and demand side (users/procurement authorities).

---

11 http://oxforddictionaries.com/definition/synergy.

12 The focus of the project is on product technologies rather than on process technologies. The latter has received much attention in earlier studies on civil-military integration, see for example: National Research Council (NRC), "Equipping Tomorrow's Military Force: Integration of Commercial and Military Manufacturing in 2010 and Beyond", National Academy Press, Washington DC, 2002.

Consequently, their design tends to be specialised and reflects particular concepts of operation and very specific user requirements;

- "Equipment and sub-systems" occupy a middle position between these two levels in terms of synergy potential;
- The three fields are likely to require different policy instruments to increase synergies.

This framework can be illustrated by the diagram in Figure 1.1.

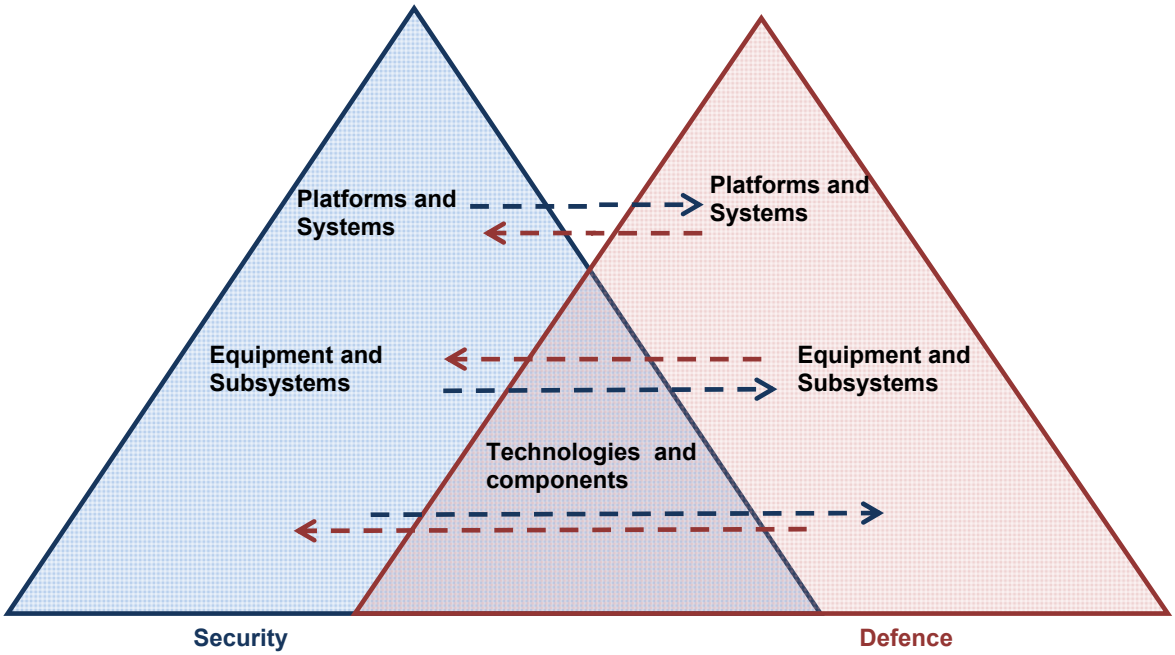


Figure 1-1. Conceptual Framework – increasing the "common space"

1.3 Case Studies and Technology Areas with high spin-off Potential

Case studies

Since there is no statistical data on spin-off activities, a case study methodology was used as the main method to analyse the context and factors that determine outcomes of the spin-off process. While the analysis of an individual case does not allow drawing general conclusions, a broad selection of cases should help to identify major factors and conditions affecting spin-off process and outcomes.

The study undertook a two-stage approach. Firstly, the project team conducted a broad scan of spin-off activities between the military and civil security sectors in the last decade. The aim was to identify a significant number of spin-off cases that could provide a general understanding of spin-off activity across various functional areas, technology levels and commercial development stages. The broad scan involved a review of previous studies done in related areas, various comprehensive listings of security, defence and dual use technologies, publications in trade magazines, review of projects in the security field under the Seventh Framework Programme, expertise of project partners and interviews with representatives of security and defence companies. The scan was conducted through systematic search across various functional areas, technology levels and commercial development stages to get a broad understanding of the dynamics and issues related to military-civil security. Secondly, an in-depth analysis of ten selected cases was carried out. This analysis helped to get better understanding of the main factors affecting the success of spin-offs between two sectors.

The charts below illustrate the distribution (mapping) of the cases that came out of the broad scan. Figure 1.2 shows that most of the spin-off activity identified took place within the functional areas: “Sensors” and “Command, Control and Communications” (C3), and “Platform integration and networked capabilities”. Figure 1.3 illustrates that spin-offs more frequently occur from the military to the civil security domain than the other way around. This should not be very surprising since capabilities and systems to raise situational awareness are essential in both domains; and that R&D expenditure in the security sector is significantly smaller than in the military domain.

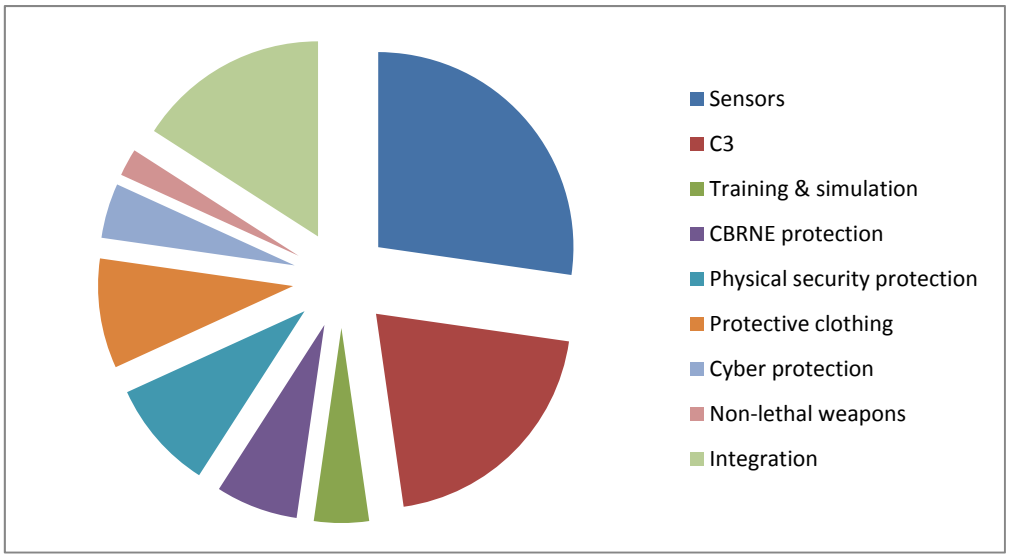


Figure 1-2. Distribution of cases per functional area

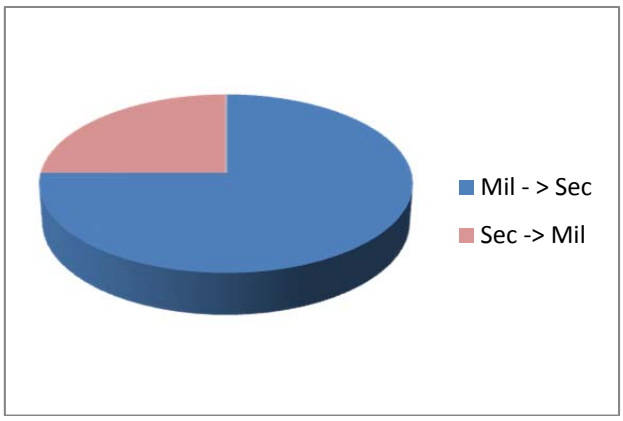


Figure 1-3. Distribution of cases by spin-off direction

Based on the in-depth analysis of selected cases, the project team identified the following main lessons that should be taken into account when seeking to influence and stimulate spin-offs between the military and civil security domain.

Lesson 1. Overlapping ‘low end’ military and ‘high end’ security missions open many opportunities for military- security synergies (spin-offs).

The case studies show that the overlapping (or blurring) security and defence missions create opportunities for using products/technologies previously unique to one domain in the other. In many cases new security threats created demand for advanced technological solutions often borrowed from defence.

Lesson 2: However, the defence and civil security markets differ significantly and the differences pose significant barriers for (potential) spin-offs

Despite the overlap between defence and security missions, the defence and security markets remain significantly different. One fundamental distinction that comes out of the case studies concerns the driving forces of technology and product development in these markets. The military market is primarily driven by performance maximization: systems and technologies used by military actors must outperform those of adversaries. New defence systems often push the technological frontier forward, with cost concerns playing only a secondary role. The environments within which the military are supposed to operate require more extreme specifications and standards (environmental parameters such as temperature, moisture, vibration, g-force, etc.). In contrast, the security market is much more concerned about cost containment.

Most of the time products developed for one market cannot be used directly in the other. For defence products, the main barriers include very high acquisition and maintenance cost, use of specialized military specifications, and somewhat less regard for comfort, safety and health standards and regulations. Security (and more generally civil) technologies often have to be ruggedized, made more secure and interoperable with the existing military technologies. The extent of the technical changes required for spin-offs varies on a case-by-case basis.

Besides technical adjustments that potential spin-offs might require, companies that want to enter a new market face additional 'soft' barriers. One issue that was pointed out in the interviews is that the required marketing capabilities differ significantly for the two markets. Even large defence companies seem to have been challenged in understanding civil security customers needs and requirements, building networks and marketing strategies This is also true for the other side – idiosyncrasies of the defence market make it difficult for civil security companies to enter the defence market; this is probably especially true for smaller companies.

Lesson 3: There have been rather few products deliberately designed for both markets from the outset (preconceived spin-offs)

We rarely encountered technologies that have been developed with both the civil security and military markets in mind. Many of the spin-off cases appear to be opportunistic: companies do not seem to design products for both markets, but do jump on the opportunity when a prospect appears for selling a technology (or an adapted version of it). One reason for a limited number of preconceived spin-offs might be directly related to Lesson 2 – large differences between the markets: it might be difficult to design for both markets simultaneously especially at the platform and system level.

Lesson 4: Spin-off from military to civil security markets is more prevalent than the other way around

Given the fact that governments' defence R&D budgets typically are significantly higher than the corresponding public expenditure on civil security R&D it is not surprising to see more spin-offs from military to civil security than in the opposite direction. Defence R&D effort leads to the development of a plethora of innovative defence products that may later trickle down to security markets.

There is also a significant flow of spin-offs from the civil (commercial) industry in general to defence. This flow is encouraged by several European MoDs that have encouraged wider use of 'off-the-shelf' components in the last decades. However, the role of the civil security industry in this flow is limited.

Lesson 5: Government regulation is often one of the main barriers for realizing spin-off potential

While government regulation is often a significant demand driver for security products case studies also show that regulation can be a significant barrier for spin-offs in some instances:

- **Health, safety and privacy regulation.** Civil security products typically have to comply with more stringent requirements with respect to comfort, safety, health and privacy compared to military products. Military products often must be extensively modified to conform to such regulation requirements.
- **Trade protectionist measures**. Defence and security industries are typically considered as strategic industries by governments. In order to protect their home industries many governments have rules that require the use of domestic production and materials for public procurement in the fields of security and defence.
- **Export control regulation**. Lengthy and costly procedures associated with export licensing significantly increase time to market and add to product cost. In addition, predictability and visibility of the criteria used by relevant authorities are often lacking.
- **Sensitivity and secrecy of defence and security technologies**. Governments adopt stringent rules to protect their technological advantage over potential adversaries, classifying military technologies. As a result these rules might (potentially) prevent transfer of military technologies to civil security, ironically, for 'security' reasons.

Functional areas with high potential for synergies

Analysis of successful spin-off cases identified two areas, sensor systems and "C3", as the most active in recent years in terms of military-civil security spin-offs. However, this is simply a snapshot of the past. We also try to identify the areas with largest potential for spin-offs based on a more structured and forward-looking approach.

Firstly, based on the analysis of successful spin-off cases, a review of published studies and theoretical considerations, we have identified the main general factors that contributed to the success of spin-offs in the past and can be used as forward-looking criteria for the identification of functional areas with high potential for spin-offs. The following four criteria seems to provide the most valuable information:

1. Similar operational needs/requirements in both civil security and defence sectors;
2. Technology level (the highest potential is at the level of technologies and components, the lowest – at the level of platforms and systems);
3. Market attractiveness (market size and growth rate);
4. Existing joint R&D.

Then, the project team conducted a structured expert assessment by applying the above criteria to the various functional areas in order to identify those with the largest potential for spin-offs. This assessment was conducted by experts from the project consortium organizations. The two functional areas that came out as the most promising ones for spin-offs, are

- "Cyber security and protection", and
- "Sensor systems" (and in particular biometrics).

1.4 Economic/ Business Models for Developing Civil-Military Synergies

There are a number of ways (modes) through which companies may seek to diversify their activities. The 'Study on the industrial implications in Europe of the blurring of the dividing lines between Security and Defence'[13] lists the following three modes :

- **Organic diversification**: a company enters a new market/sector by drawing on its internal resources and capabilities to exploit already existing technologies;
- **Diversification through acquisition**: a company enters a 'new' market through acquiring other companies that already have relevant technologies/products and an established market position among customers in the 'new' market;
- **Collaboration (partnering, teaming and joint ventures)**: a company leverage of its own technologies or capabilities through partnering or teaming-up with other companies in order to create a complementary package of market knowledge and/or capabilities to enter a 'new' market.

In addition, technology synergies may also be realised by a company without directly entering a new market:

- **Third-party mechanism (e.g. technology licensing)**: a company leverage of its own technologies or capabilities through partnering or teaming-up with other companies in order to create a complementary package of market knowledge and/or capabilities to enter a 'new' market.

A firm seeking to pursue a technology-based spin-off must obviously possess a technology that corresponds to the common needs of both sectors. Accordingly, for example, there is no basis for defence companies to enter the security sector unless they possess technologies that correspond to the needs of the security sector. The company's technology should also have some competitive/commercial advantage over its competitors.

There are also other aspects that may be required for a technology to be successfully transferred from one sector to another. These include, for example compatibility with existing skills (e.g. whether users in the new market have the required skill set to use a technology effectively or if substantial training is required), existing practices (e.g. operational doctrines and modes of operation), existing organisational processes (e.g. potential disruption to business processes that may be caused through adoption of the technology), and values and norms of potential adopters (e.g. safety, privacy, data protection and other similar issues)[14].

The case studies tend to indicate that synergies (technology 'spin-offs') have occurred more through serendipity than as a result of systematic business approaches aimed at generating technology synergies between the security and defence sectors. Given the relatively short timeframe over which the civil security sector has taken on its present form, it is necessary to be somewhat cautious in drawing conclusions on the potential for future synergies on the basis of observed past behaviour. Further weakening of the separation between military and civil-security missions and capability requirements should a priori provide an increased rationale and greater opportunities for technology-related synergies between the two sectors. However, it appears that

[13] Istituto Affari Internazionali (IAI), IRIS and Manchester Institute for Innovation Research, *Study on the industrial implications in Europe of the blurring of dividing lines between security and defence*, 2010, study commissioned by DG Enterprise & Industry.

[14] Ibid.

even large defence and aerospace contractors have found it difficult to leverage technology developed for one market (typically, but not exclusively, defence) for applications in the other sector and firms find it difficult to integrate the potential for such synergies into business decision making processes.

Overall, the significant differences in the structures of supply and demand in the security and defence sectors hinder the development of common business approaches to the two sectors and for companies with business models developed to operate in one market environment to enter into the other market. For companies that are familiar with the more coherent and strategic approach in the defence sector, significant adjustments to their business strategies may be required to accommodate the more fragmented and amorphous conditions in the security sector. For companies operating in the security domain – or, for SMEs technology suppliers in general – the general structure and procurement arrangements and cycles are seen as factors inhibiting access to the defence sector. Further, the controls and limitations that governments may place on the exploitation of technologies for non-defence purposes is also seen as an important consideration for technologies with potential applications in both areas, particularly where the size of the defence market is relatively small compared to civil (including civil security) markets.

One of the most significant factors to inhibit industry stakeholders from developing coherent business approaches to spin-offs between the security and military sectors is the absence of a 'top-down' approach for identifying capability requirements and technology needs in the security sector. The development of a longer term vision and 'roadmap' for security technology requirements that could be set alongside those developed for the defence sector would enable potential areas for technology synergies to be identified, together with a better appreciation of overall market potential. Overall, this should reduce the level of uncertainty attached to industry efforts to develop or adapt technologies for the respective markets, in particular the security market.

There is general consensus among industrial stakeholders consulted for this study that greater clarity of security market technology requirements and expected demand levels, together with clarity and openness of the processes and procedures for accessing markets ('route to market'), would encourage industry to more systematically integrate the potential for technological spin-offs into its business strategies. Under such conditions, other possible policy initiatives that may be considered to support the promotion of synergies between security and defence (e.g. standards, R&D funding programmes, etc.) would be more likely to have a positive effect.

1.5 Policy Options and Impact Assessment

Policy Options

The study team has carried out an impact assessment of the four policy options proposed by the Commission for enhancing civil-military synergies:

1. *More systematic coordination of research activities between FP7 and EDA through the European Framework Cooperation.*

   This option assumes that the European Commission and EDA will continue to coordinate research activities through the European Framework Cooperation for Security and Defence (EFC), but in a more systematic way than is the case today. As of today the EFC only covers CBRN. This option implies a significant increase in the number of joint or coordinated research projects across many functional/technological areas.

2. *Improved upstream coordination at the level of capability development through high-level stakeholder group;*

   A high level stakeholders group would incorporate the main actors from the supply, demand and end-user side from both the civil and the military sectors. The aim of such a group might be to identify those areas where common requirements for civil security and military end-users could be set, and common research, development and procurement initiated. This identification process might lead to synchronized projects under EFC, or to establishing areas where standardisation might be beneficial. Establishing a high level stakeholder group could accompany several of the other options described here.

3. *Downstream coordination via development and use of 'hybrid' standards;*

   Under this policy option, the Commission could take the lead in formulating and establishing European standards in some or possibly many functional areas, and in promoting the use of those standards in both the civil security and military domain. In general, synergies between civil security and military domain could be fostered by standardisation at the technical, architectural and organisational level.

   At the technical level (technical interoperability standards) [15] this policy option should be aimed at the interaction between defence and civil standards in general. Standardisation at the organisational level (organisational interoperability standards) should aim at achieving greater interoperability between civil security and defence organizations via harmonisation of corresponding protocols, procedures and guidelines. This will stimulate conformity between the two domains at the level of capabilities and may help to overcome fundamental differences between the two domains, thereby facilitating synergies. Standardisation or, more appropriately, harmonisation at the architectural level, where distributed functionality can be linked together in (both physical and logical/functional) networks, could drive synergies at the lower level since it can only be fully achieved with technical and organisational interoperability standards in place.

4. *Use of Article 185 TFEU[16] to support joint research effort.*

   Implementing Article 185 TFEU in the 7th FP implies that participating EU Member States integrate their research efforts by defining and committing themselves to a joint research programme, in which the EU promotes the voluntary integration of scientific, managerial and financial aspects. The EU provides financial support to the joint implementation of (parts of) the national research programmes involved, based on a joint programme and a dedicated implementation structure.

Results of the impact assessment

The assessment has been based on information obtained from stakeholder interviews, case studies, and a number of literature sources, complemented with a causal chain analysis. In line with the Commission's Guidelines for impact assessment, the economic impacts and social impacts were addressed.

The impacts were assessed for three main stakeholder groups:

1. Impacts for industry: the producers of civil security and military products;

---

[15] European Commission, Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards, M/487 EN, Brussels, February, 2011.

[16] Article 185 TFEU states: "In implementing the multiannual framework programme, the Union may make provision, in agreement with the Member States concerned, for participation in research and development programmes undertaken by several Member States, including participation in the structures created for the execution of those programmes."

2. Impacts for users: the end users of civil security and military products;
3. Impacts for society as a whole.

The four policy options were compared against the baseline situation, which reflects the current situation and assumes no significant (new) policy intervention. For the analysis of impacts, the baseline is characterised as follows: Synergies continue between civil security and military markets and vice versa as before. The majority of spin-offs go from the defence sector to the civil security sector. An initial assessment for five subsectors indicates unused potential of around €2.2 billion of sales between 2010 and 2020. European policy on civil-military synergies consists of the continuation of the European Framework Cooperation between the European Defence Agency, the European Commission and the European Space Agency

The main result of an overall assessment is that the option of the deployment of Article 185 will have the most substantial impact. The option will lead to more available public R&D funding (which is also an administrative cost), which should lead to more spin-offs and extra sales for industry. The option on the improved EFC also brings about significant impacts in the form of reduced duplication and a better probability for successful spin-offs. The impact of hybrid standards is potentially large, however, the voluntary character on the adoption of the standards makes it uncertain if these standards will be adopted and thus if this potential is ever realised. Finally, the option of the High level Stakeholder Group leads to slightly positive impacts, but does not make a direct link to an increase of sales or reduced duplication of effort. As such, it seems more as a 'no regret' option: it favours some of the conditions for improved spin-off potential and does not cost a lot. These results are summarised in the table below.

The table should be read as follows. The second column describes the impact, and the first column indicates if this impact is positive (+) or negative (-) for that stakeholder. The signs in the columns under the policy options shows how that policy option affect an impact, i.e. whether the impact becomes more positive (+) or negative (-) for that stakeholder. As an example: the increase of marketing costs is in itself a negative issue for a stakeholder. In option 2-4 this impacts becomes more positive for the stakeholders (+), i.e. their marketing costs decrease.

Table 1-1 Overview impact of given policy options

	Impact	Option 0	Option 1	Option 2	Option 3	Option 4
		Baseline	Improved EFC	Hybrid standards	High level SH group	Article 185
	Industry					
+	Increase R&D expenditure {E}	0				
-	Increase marketing costs {E}	0		+	+	+
+	Increase of sales {E}	0	+	+	0/+	++
+	Increase of R&D success {E}	0	+		0/+	
+	Reduction duplication of R&D efforts {E}	0	+		0/+	
+	Increase of available R&D funding {E}	0				+
+	Reduction market fragmentation {E}	0		+	+	+
	End users					
-	Increase of procurement costs {E}	0	-	-	-/0	-
+	Decrease of procurement costs	0	+	+	0/+	+

	{E}					
+	Improved cooperation between civil security and military end users {S}	0	+	+	+	+
+	Improved cooperation between civil security end users {S}			+	+	+
+	Improved cooperation between military end users {S}					
	Society	**0**				
+	Increase employment {S}	0	+	+	0/+	+
+	Increase security {S}	0	+	+	0/+	+
	Other					
-	Increase admin costs {E}	0	-	-	-	--
+	Reduced duplication of efforts {E}	0	+		0/+	+
	Overall score					
		0	+	+	0/+	++

E = economic impact, S = social impact.

Other policy options

The policy options described above only partially address the structural barriers for increased synergies . One of the main barriers for creating synergies between the defence and the civil security domain is the lack of a longer term perspective and technology roadmaps in the security domain. Development of such a perspective is primarily a national level responsibility. Indeed, a number of national initiatives are under way to address that barrier. Some Member States have started a process of developing some sort of "capability based planning" approach, similar to the one cultivated in the military domain over many years. In addition, these MS have started comparing military and security capacity development plans and are looking for shared road maps to delineate dual technology needs. This sort of efforts can be seen, amongst others, in France, the United Kingdom and the Netherlands[17]. Such national initiatives on military-civil security synergies indicate that, despite obvious difficulties, conditions exist for implementing a meaningful policy reform in the field. A first alternative policy option would be for the Commission to coordinate with the Member States that have already launched concrete initiatives, for example, by facilitating exchange of best practices and lessons learned. The Commission may also take the lead in initiatives that would stimulate a 'Capability Based Planning' approach for civil security mission areas where the EU has political and operational responsibilities, such as FRONTEX.

A second alternative policy option could be to streamline regulation. Regulation plays an important role, for example, in promoting standards. Such standards should be established in the interplay between regulators and market parties. A high level stakeholder group may play a pivotal role, for example in establishing organisational interoperability standards.

Another important area is health and safety regulation, which lies at the national and the EU level. For some spin-off examples existing regulation clearly forms a significant barrier. Revisiting existing regulation might be beneficial, but it should be done only a case-by-case basis since such regulation has a very important role in the society.

[17] For example, UK Ministry of Defence, "National Security through Technology: Technology, Equipment, and Support for UK Defence and Security" (Cm 8278), February 2012.

A final suggestion was for the European Commission to consider the establishment of a European industrial database of available dual use technologies in Member States and R&D projects on technologies and products being developed for civil security and military application in the Member states and at the European level. This would better inform industry concerning available technology in other Members States, to include in further product development across the two markets. Such a database could lower the walls between the markets, and reduce duplication of efforts.

1.6 Recommendations

Summarizing the results of the study we think the European Commission could consider several policy measures to foster military – civil security synergies. The following recommendations are based on the analysis done by the project team and do not represent views of the Commission or are in any way binding the Commission:

Recommendation 1. The Commission could promote best practices with respect to a 'capability based approach' for civil security amongst the MSs, building upon various national initiatives already under way. This should lead to a process of establishing shared defence-security technology and capability road maps and, eventually, joint R&D efforts to implement these roadmaps.

Recommendation 2. The European Commission could look at ways to use EFC to promote the establishment and implementation of shared defence-security technology and capability road maps.

Recommendation 3. The European Commission could look at ways to promote best practices and technical / organisational interoperability standards as a solid basis for and element of the process of establishing shared defence-security technology and capability road maps.

Recommendation 4. The European Commission could use 'Article 185' established as an instrument to bring together interested MSs for joint R&D efforts as part of shared defence-security technology and capability road maps.

Recommendation 5. The European Commission could consider establishing a high level stake holder group as a way to create more favourable conditions for and stakeholder 'buying-in' of implementing the other recommendations.

Recommendation 6. Next to stimulating national initiatives already under way (recommendation 1), the European Commission could explore the possibility of shared defence-security technology and capability road maps for mission areas for which the EU has political and operational responsibilities, such as FRONTEX.

2 Context

2.1 Background

Key security threats to Europe have changed dramatically over the last two decades. While the risk of large-scale aggression against any member of the European Union (EU) has become

exceedingly low, other threats have gained in importance. The European Security Strategy "A Secure Europe in a Better World" adopted in 2003[18], lists as key threats:

- Terrorism;
- Proliferation of weapons of mass destruction (WMD);
- Regional conflicts;
- State failure;
- Organised crime.

Where the European Security Strategy focuses on military and external threats, the EU Internal Security Strategy presented early 2010[19], deals with civil security threats and aims to integrate security actions in the following seven domains:

- Terrorism;
- Serious and organized crime;
- Cybercrime;
- Cross-border crime;
- Violence itself;
- Natural and man-made disasters;
- Other common phenomena which pose European wide safety and security threats such as road traffic accidents.

The overlap of key threats identified in these two strategies points to an increasing convergence in threat identification, analysis and policies in the civil security and military domain. Traditionally, security risks were divided into external risks, i.e. originating outside the territory of the state, and internal or domestic risks. The former was the domain of military, the latter of civil (non-military) security forces. However, new types of security threats do not fall neatly into one of these categories. They are more diverse, more uncertain and less visible than, for example, the threat of global military confrontation during the Cold War. Threats from large and sophisticated terrorist organizations operating across international borders involve both external and internal security dimensions and addressing them often requires close cooperation between internal security services and armed forces. Indeed, the European Security Strategy emphasizes that "none of the new threats is purely military nor can any of such threats be tackled by purely military means alone". Instead, they call for a mixture of instruments and close cooperation between the military and the security domains.

These developments clearly indicate that dividing lines between defence and security are becoming much less clear cut (see the 2010 Report of the 'Study on the industrial implications in Europe of the blurring of the dividing lines between Security and Defence' – hereafter IAI, 2010). Modern missions of the defence and security forces such as crisis management and border protection are often closely interlinked.[20] This presumably should have significant implications for the capabilities and systems required to perform such missions, hence for defence and security industries to develop and deliver such systems..

However, the security sector has not received much attention from the competitiveness and industrial policy perspective despite the fact that security policy has taken a much more important role in government priorities and that considerable effort has been devoted to improve security-

---

18 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/reports/78367.pdf.

19 http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

20 The study referred to in footnote 3 notes that the degree of blurring between security and defence is much more pronounced at the theoretical level, in terms of missions and functions, while at the operational level it remains more limited and often not non-existent (p. 61).

related research capabilities. The EC Communication “An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage”[21] pays special attention to the security industry: “The EU security industry faces a highly fragmented internal market and a weak industrial base. National regulatory frameworks differ widely and the market for security products is highly diversified, ranging from cameras to complex scanner systems. [...] It is essential to develop a fast-track system for approval of priority technologies; to make substantial further progress on harmonisation, standardisation; to consider coordinated public procurement; and to accelerate R&D on security technologies.“

Within this context, one option to strengthen the industrial base is to (further) enhance and strengthen cooperation between the civil security and military domains. Bringing the two domains closer together with respect to demand formulation (capability requirements) and supply propositions (technology and systems development) this option might expand the market for both defence and security companies and reduce unnecessary duplications.

Another factor that makes increasing cooperation between the defence and civil security industries important is on-going and expected reductions in public expenditure in most of EU countries. Many European countries will have to implement significant fiscal adjustments to stabilize and reduce their public debt. Stricter budget constraints suggest that public expenditure on procurement of civil security and military equipment might be smaller in the near future. Policy options that promote spin-offs between civil security and defence could help to save public money and contribute to the rationalization of the corresponding industries.

The financial pressures after the end of the Cold War were a major incentive for the military to move to a more extensive use of commercial technologies and equipment in the defence systems (the other main reason was technological leadership of the commercial sector in several key technological fields, such as information technologies). The use of commercial off-the-shelf (COTS) products in the military field can be seen as a general case of the spin-offs from the civil (commercial) sector to the defence sector. Advantages and disadvantages of the greater use of COTS items in military are discussed elsewhere in the literature (U.S. DoD, 2000; NRC, 2002c; DSB, 2009). This literature provides a very helpful review of the main issues associated with the use of COTS equipment in defence systems as well as the barriers for greater use of commercial technologies in military. The current study draws on some of the lessons identified in this literature.

The current project continues recent efforts undertaken by the European Commission (EC) to provide better understanding of the security industry, to analyse the impact of new security threats on the industry and to develop policies to strengthen the internal security market. The particular purpose of this study is to improve the understanding of the extent and the nature of synergies between civil security and military domains. It identifies recent cases of technological spin-offs between the two sectors and analyses the main factors affecting the spin-off process. The study also evaluates policy options intended to remove barriers and to provide incentives for an enhanced flow of such spin-offs.

2.2 Definitions

To ensure consistency and common understanding, especially in the area where multiple terms with a similar meaning are widely used, it is important to discuss terminology at the outset of the

[21] COM(2010) 614.

report. The title of the project refers to civil-military synergies in the field of security. In a general sense, a synergy can be defined as "the interaction of two or more organisations [..] or other agents to produce a combined effect greater than the sum of their separate effects".[22] In the present context a civil-military synergy implies greater effectiveness or efficiency is achieved through combined actions or cooperation between or towards the civilian sector (or, specifically the civil security sector) and the military sector that would be achieved separately.

The study will focus on a particular form of synergy between the civil security and military sectors: technological spin-offs (in both directions) between these sectors. We understand a "spin-off" to be the application of a technology developed primarily for one sector in the other sector. Since synergy is a very broad term, in this report we will use the term "spin-offs" ("spin-ins", being a mirror image of "spin-offs").

This definition places spin-off close to "technology transfer", although the term takes on different meanings for different authors. Other terms sometimes used in a similar context are "dual use" and "bridging technology". The term dual use is defined in Council Regulation No 428/2009, which regulates the export of dual use technologies to third countries: "Goods and technologies are considered to be dual-use when they can be used for both civil and military purposes". Because this term is strongly linked to export regulation, the Terms of Reference for this study suggests using the term dual use only in the export related context and "bridging technology" in other circumstances. To ensure consistency we will use the term "spin-off" throughout this report instead of other similar terms.

Spin-offs could be both incidental (not pre-planned) or preconceived (by design or on purpose), although in practice the distinction between them is often unclear. Spin-offs between various sectors are abundant in the modern economies. An ultimate example of such spin-offs is general purpose technologies that affect an entire economy (e.g. IT-related technologies). The use of COTS items in defence systems is another example.

"Technology" - as in "technological spin-offs" - is also a very broad term. We distinguish three different technology levels[23]:

4. Integrated platforms and systems;
5. Equipment and sub-systems;
6. Technologies and components.

In this study a broad range of spin-offs across all technology levels has been analysed to get a comprehensive picture of such spin-offs and the factors contributing to or impeding synergies between military and civil technologies.

2.3 Conceptual framework for civil security – military synergies

As mentioned, the growing importance of non-military threats is reflected in the fact that the dividing lines between security and defence in terms of missions and capabilities are often becoming blurred. The evolving nature of the relationship between defence technologies and security technologies is also noticeable in the field of Research & Development, as new technologies show potential for both areas. There are opportunities to avoid duplication and strengthen

[22] Oxford Dictionaries: http://oxforddictionaries.com/definition/synergy.

[23] The focus of the project is on product technologies rather than on process technologies. The latter has received much attention in earlier studies on civil-military integration, see for example OTA, 1994, NRC, 2002c.

complementarities and co-operation in specific areas where technologies can have civil and defence applications. To this end, there have been numerous calls by the European Council to foster synergies between security and defence technologies[24], with potential benefits such as:

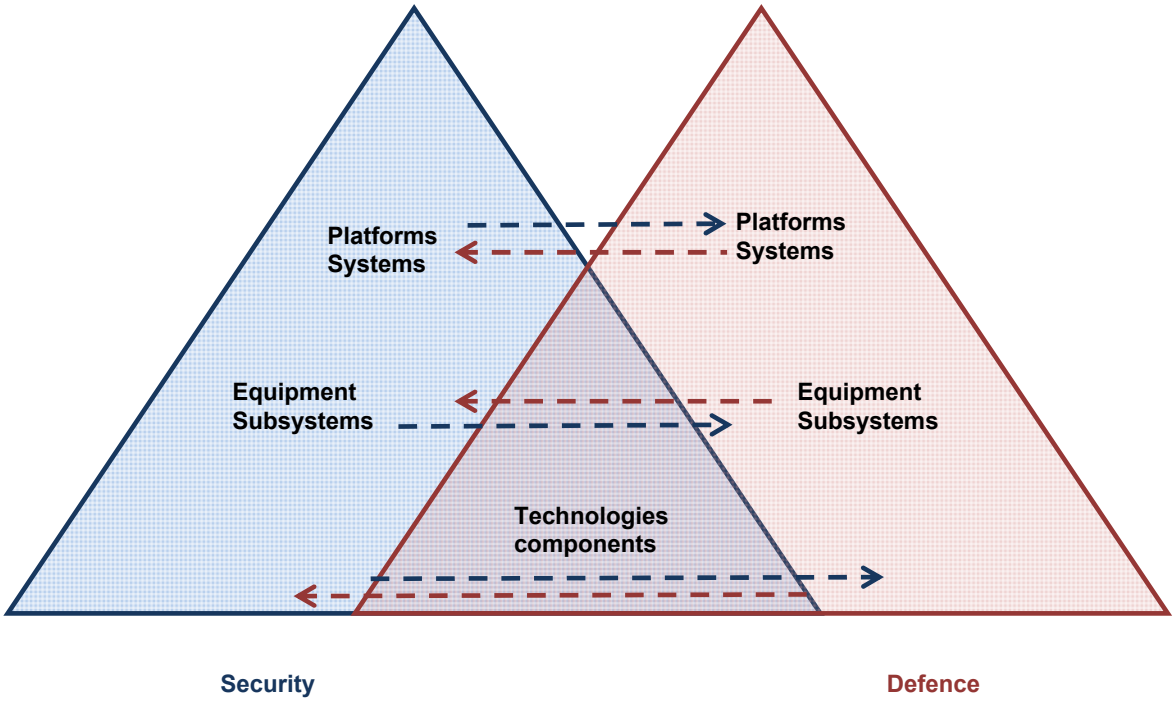
- Increased flow of spin-offs may offer a potentially larger and more integrated market for both defence and security companies. This will strengthen the industrial base and offer cost savings in public procurement of defence and civil security equipment and systems;
- Technological spin-offs between the civil security and military sector strengthen the competitiveness of European companies in a global context;
- Strengthening European capabilities in generic technologies will have benefits for civil, security and military spheres, especially for areas where dependencies on non-European sources are to be prevented.

This study focuses on options to maximise spin-offs and addresses two questions:

- What are factors that facilitate and/or hinder spin-offs?
- Which, if any, of these factors can be addressed by the Commission through industrial policy actions?

We propose the following conceptual framework to address these questions (see Figure 1.1).

Figure 2-1 Conceptual Framework – increasing "the common space"



This conceptual framework emphasises the following points:

- Three technology levels have different innovation dynamics, as well as differences in the demand side and supply side. This leads to differences in the potential synergies that might be expected;
  - "*Technologies*" are essentially "neutral", in the sense that technologies are not inherently military or civilian, their applications are specific. Thus, our conceptual model considers technologies as being generic and having application across a wide variety of civil, security

[24] See: http://www.ess-project.eu/news/83-the-european-council-insists-on-development-of-civil-military-synergies.html.

and military areas. Critically, where technologies originate (whether it is the defence or civil industry) influences the ways and possibilities of their diffusion and use;
  - For (integrated) "*systems/platforms*" the potential for synergies tends to be most difficult to bring to fruition. The design and specification of systems/platforms emerge from a close relationship between the supply side (companies) and demand side (users/procurement authorities). Consequently, their design tends to be specialised and reflects particular concepts of operation and very specific user requirements;
  - "*Equipment and sub-systems*" are in between these two levels;
- The three fields are likely to require different policy instruments to increase synergies.

Several steps have already been taken to promote spin-offs between the civil security and military fields. The European Commission and the European Defence Agency (EDA) have started some form of cooperation through the European Framework Cooperation (EFC). The focus is to create synergies between the civil security research programme of FP7 and EDA's defence research activities. However, there is no systematic cooperation at the level of capability development[25]. Therefore, research cooperation remains difficult, as long as there is not a more fundamental understanding between Interior Ministries and Defence Ministries in Europe about required capabilities. Furthermore, such synergies appear to be hampered by the fact that the outcome of research projects is not used to undertake coordination at the level of standards. Such coordination would seem to be useful and cost-effective in certain areas (such as, for example, unmanned aerial systems and software defined radio (SDR)).

Some previous studies have made attempts to identify areas with potential for spin-offs. For example, the European Security Research Advisory Board (ESRAB) has listed priority technology areas for security research, that partially overlap with areas important for defence applications[26]. A recent study "*The industrial implications of the blurring of dividing lines between defence and security*"[27] also identifies technologies with promising prospects for applications across defence and security missions.

A particular area that provides a clear evidence of the increased technology transfer between civil (security) and military sectors is "Space". The European Space Agency (ESA), EDA and the Commission are closely cooperating on a variety of subjects, including intelligence, surveillance and reconnaissance, satellite communication in support of unmanned aerial vehicles (UAV), and space situational awareness, as well as critical space technologies. ESA and EDA recently signed an Administrative Arrangement to better support Europe's security and defence needs[28]. For this purpose a lot of work has already been done to map and stimulate possible synergies between civil (security) and military sectors in the Space realm. Therefore, and with the Commission's approval, for this project space-related activities have been excluded from its investigations and analysis.

---

25 In fact, even the understanding that there is a need for "capability development" is much less common on the civil security side as it is on the defence side. Also, the "institutionalised cooperation" between European MoDs on capability development is missing in the civil security sector, perhaps with some exemptions.

26 James, A., Defence and Security R&D in Europe. SANDERA Background Paper, 2009.

27 Istituto Affari Internazionali, IRIS and Manchester Institute for Innovation Research, Study on the industrial implications in Europe of the blurring of dividing lines between security and defence, 2010, study commissioned by the EC. Available at http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf.

28 http://www.esa.int/esaCP/SEM762E1XOG_index_0.html.

2.4 Differences between the civil security and defence markets

The *defence sector* in Europe, commonly referred to as the European Defence Technological and Industrial Base (EDTIB) can be demarcated relatively easily[29], even if it consists of sub-sectors that have very different industrial, technological and market characteristics and different military requirements.[30] The demand side is clearly defined: the end-users of military products and services are almost entirely made up by national Ministries of Defence (MoDs). This concentration on the demand side is to a large extent reflected on the supply side as well. Lead systems integrators, platform producers and producers of weapon systems are mainly large companies, primarily "national champions", specialized on defence production. These so-called 'prime' contractors subcontract specialised systems producers, for example in electronics, and producers of complete sub-systems or major components. Often, these 'tier 1' contractors are also risk sharing partners. Although few of these prime and tier 1 companies only produce for the defence market, they are very much aware of their status as defence companies and are fully organized to the particular characteristics of the military market. From the clear and focused structure on both the demand and the supply side, it follows that the interaction between the two sides is both well regulated and intimate. Established, long term relationships are important. This situation constitutes a significant barrier for new entrants to the defence market.

From a technological point of view, the defence sector is characterized by a long term and integrated approach, often caught under the term "capability based planning". The various MoDs across Europe typically clearly and firmly establish military requirements for the longer term. Military equipment typically has a life of several decades. In many cases, the defence industry is involved in defining the technical specifications for equipment that are derived from these requirements. The demand side is prepared to share risks in technology and platform development. Although the influx of 'civil' technology has increased over the past decades and will continue to do so, the defence technological base is still quite clearly defined. Again, this forms a barrier for new markets entrants, in particular innovative SMEs.

In marked contrast to a firmly established defence sector, the scope and perimeters of *the security sector* are highly amorphous. The concept of a civil 'comprehensive security' domain has only taken shape over the last decade or so. This conceptual idea of a (more or less) cohesive domain spanning elements of security that in the past were largely disconnected, is only partially reflected in the real world. Despite some national initiatives to develop a more structural and long term approach, the demand side remains very fragmented. Its core typically consists of the Ministry of the Interior, that typically has lead responsibility for national security, and of various auxiliary services and security agencies. Increasingly other ministries and operational organisations also have a stake in comprehensive security (whole-of-government approach); as do citizens, private industry and societal organisations (whole-of-society approach, societal resilience). Many of these stakeholders are not used to formulate their needs in terms of functional requirements and capabilities over a longer period of time, let alone consolidate these in a joint vision and strategy. The fragmentation on the demand side is mirrored on the supply side, which is neither well defined nor clearly identifiable in terms of recognised classifications of industrial activities.31 Unsurprisingly, the sector lacks clearly defined and shared technology roadmaps which, in turn, impedes structural and substantial technology investments.

---

29 TNO, Development of a European Defence Technological and Industrial Base, 2009, study commissioned by DG Enterprise & Industry.

30 Manchester Institute of Innovation Research and Centre for Defence Economics, Study on How to measure Strengths and Weaknesses of the DTIB in Europe, 2008, study commissioned by EDA.

31 ECORYS, DECISION and TNO, Study on the Competitiveness of the EU security industry, 15 November 2009, study commissioned by DG Enterprise & Industry.

Furthermore, the security technological base is not very distinctive. Many technologies in the security field are applicable across different sectors (for example, protective clothing, secure and mobile communication, IT and network security, etc). As a result, many security sectors to a large extent overlap with the safety and other civilian industries, which often leads to widely different definitions of the security industry and estimates of its size. R&D expenditure in the security industry is significantly smaller than in the defence industry, notably because of a stronger focus on cost containment, the lack of 'mass' on both the demand and the supply side, as well as of longer term (shared) visions as the driver for technology roadmaps.

Summing up, the defence and civil markets have significant differences. These differences include:

- Demand side: consolidated and public for defence, fragmented and public and private for civil security;
- Supply side: clearly demarcated for defence, blurred for civil security;
- Interaction between demand and supply: well structured and centralized for defence, decentralized and locally structured in security;
- Technology and product development: longer term technology roadmaps and cost and risk sharing drive innovation for defence, little dedicated innovation for security.

3 Aim and Approach

This Chapter describes the project approach. The project has been organised around several distinct activities. One group of activities has focused on case studies of technological spin-offs between the defence and civil security sectors (in both directions). Another set of activities deals with more general and theoretical issues related to the spin-off process. More specifically, the study includes identification of the functional areas with the highest potential for spin-offs and deals with the economic models used by economic agents in evaluating potential spin-offs. Finally, the report discusses industrial policy options for the security sector and provides an impact assessment for them.

3.1 Aim and objectives

Aim

The aim of the study is to get a comprehensive overview of the existing (and potential) areas for enhanced civil-military cooperation. Based on existing synergies between the civil security and military sectors (spin-offs/spin-ins), as seen over the last ten years and with a focus on Europe, the study identifies technological areas with the highest potential of synergies and provides criteria used for such assessment. This includes economical models that might be used by industry to identify such areas of interest.

Based upon this analysis, it provides options to further strengthen synergies between the civil security and military sector, in particular the possibility of “hybrid standards” and the creation of a “high level stakeholders group on civil/mil synergies”. An impact assessment of these options is part of this analysis.

Objectives and Tasks

This leads to the following tasks and objectives:

- **Case studies**: identify cases that illustrate successful areas of spin-offs / spin-ins over the last ten years between the security sector and the defence sector in Europe, with an overview of the criteria to assess the successfulness of these cases;
- **In-depth exploration of selected case studies**: this task aims to provide a deeper understanding of the factors involved in the spin-off process, barriers and driving forces at the Commission’s request. Some cases are to be explored in more detail to develop an initial insight in the quantitative effects of actual spin-offs. This exploration serves as a first contribution to the Commission to illustrate the potential of the main policy options the Commission considers;
- **Technological areas with high potential for spin-offs**: identify the most promising areas for spin-offs / spin-ins between the civil security and the military sector, with an overview of the criteria used as a basis for this assessment (with the selected cases mentioned above being part of the assessment). In doing so, close attention will be given to the ethical aspects of the possible synergies between civilian and military technologies;
- **Economic models**: identify economic models used by the industry to select areas of interest for civil-military spin-offs/spin-ins;
- **Impact assessment of the main policy options**: conduct an impact assessment of the main policy options that might help strengthen synergies between the civilian and the military sector;

- **Additional policy options:** briefly describe additional policy options that may have emerged as a result of the case studies and consultations with stakeholders and experts.

3.2 Taxonomy of functional areas

The selection of an appropriate taxonomy is an essential element of this study. Such taxonomy helps to organize and structure the data collection and to classify and compare findings in a systematic way. The defence industry has well-developed and established taxonomies, for example, the EDA technology taxonomy for defence technologies and product/systems.[32] This cannot be said for the security industry. It is very fragmented and is not well structured, which makes it very difficult to capture within standard industry classifications such as NACE (Statistical Classification of Economic activities in the European Community) or ISIC (International Standard of Industrial Classification).

As the main objective of this study is to contribute to an industrial policy for the security industry, it was decided that a taxonomy should reflect the security industry products and structure. The project team has looked at several schemes that bear relevance to its study, including the categorisation used by ESRIF (European Security Research and Innovation Forum)[33], ESRAB (European Security Research Advisory Board)[34], as well as the STACCATO taxonomy.[35] None of them seemed to fully meet the project's needs. In the end, the project team decided to augment the technology-based classification of the security industry presented in the *Study on the Competitiveness of the EU security industry* (referred to in §1.2):

- Sensor systems and (sensor) information processing, including:
  - Tracking and tracing;
  - Screening and scanning;
  - Biometrics.
- Command, Control and Communications (C3);
- Training & simulation;
- CBRNE protection;
- Physical security protection;
- Protective clothing;
- Cyber protection;
- Non / less lethal weapons;
- Platform integration and networked capabilities.

This taxonomy along with the technology levels (see Figure 1.1) is used to classify and organize case studies of the spin-offs.

---

32 http://www.eda.europa.eu/Libraries/Documents/Technology_Taxonomy_Description.sflb.ashx.

33 ESRIF Final Report, 2009, http://www.gppq.mctes.pt/brochuras/online/ESRIF_Final%20report_2009.pdf.

34 ESRAB, Meeting the Challenge: European Security Research Agenda, 2006, http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf.

35 STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities (STACCATO), Deliverable D 1.2.2. STACCATO Final Taxonomy, 2008, supporting activity within the Preparatory Action on the enhancement of the European industrial potential in the field of Security research (PASR).

3.3 Case studies

One of the main tasks of the project is to develop a mapping of successful areas of spin-offs between the civil security and the defence sector (and vice versa) over the last decade or so. In order to achieve this the project team conducted a systematic search for existing and potential spin-offs using a variety of sources. The search involved a review of previous studies done in this area (e.g. Chait et al., 2006; IAI, IRIS an MIIR, 2010; NRC 2002b; NRC, 2003), various comprehensive listings of security, defence and dual use technologies, publications in trade magazines, security and defence companies' web sites, analysis of projects in the security field under the **Seventh Framework Programme (FP7),** expertise of project partners and interviews with representatives of security and defence companies, research and development organizations, trade associations and end-users.

The initial allocation of work was based on the national basis with each partner focusing on a particular country based on that partner's expertise and competencies. The allocation of case studies by country helped the project team to get the most efficient use of expertise and knowledge accumulated by the project partners, as well as easy and efficient access to respective stakeholders.

However, our search quickly demonstrated that in today's world national barriers are losing importance, and it is often difficult if possible at all to classify spin-off cases on a national basis. One such example is the TenCate case. TenCate is a Netherlands-based company, but most of its protective clothing manufacturing and sales takes place in the U.S. Its "Defender M" fabric is based on fibre developed by the Lenzing Group, headquartered in Austria. We also found the United States to be a rich source of spin-off cases and omitting it from our search would provide a skewed picture of successful civil-military spin-off activities.

The result of our mapping and a broad overview of cases is presented in Chapter 3. It also includes lessons and conclusions drawn from our analysis of the identified spin-off cases.

3.4 In-depth analysis of selected cases

The mapping of spin-offs developed in the previous task served as main input for in-depth case studies of selected spin-offs. The selection of cases for in-depth analysis aimed to provide a representative sample of spin-offs. The selected cases include examples that provide a broad coverage of functional areas; spin-offs that are commercially successful and those that are still at a pre-commercial stage; spin-offs at the different technology levels – from platforms such as unmanned aerial vehicles to more basic technologies such as infrared cameras. Availability of and accessibility to information was also an important factor in selecting cases for in-depth investigations.

Analysis of a number of individual cases allows us to draw more general lessons and conclusions. One important lesson from the cases studies is that the success of spin-offs are difficult to predict given the fact that planned, direct military to civil security spin-offs (and vice versa) are not a norm; transfer of technology from one sector to the other often involves a complex, non-linear path. Identification of the factors contributing to and/or hindering the success of the spin-off process was also part of the case analysis. These lessons are essential for the identification of areas with high spin-off potential, for the development of policy options and to provide insights for the impact assessment of the proposed policy options.

At the request of the Commission the project team also undertook some in-depth quantitative case studies. The objective of these case studies is to provide an initial quantitative estimate of typical impacts associated with technological spin-offs. The estimates are meant to inform the Commission's decision-making with respect to its' security sector industrial policy. These results also informed our analysis and provided a foundation for several in-depth cases presented in Chapter 3 and contributed to the impact assessment analysis. The results of this task were delivered to the Commission as a stand-alone memorandum, and are summarised here in Chapter 7.

3.5 Functional areas with the largest potential for synergies

Functional areas with the largest potential for synergies (spin-offs) are of obvious interest to various stakeholders. One way to identify such areas is to look at the past spin-offs. Simple analysis of the identified spin-offs in Chapter 3 suggests that C3 and sensor systems were the areas with the largest number of spin-offs. However, this approach suffers from two problems. Firstly, it cannot claim statistical representativeness. Secondly and even more importantly, the past does not always serves as a good guide to the future.

The other approach that was used in Chapter 4 starts with the identification of the factors that contributed to the success of the spin-offs in the past based on analysis of the case studies, theoretical considerations and literature review. From these success factors the following main criteria were selected:

1. Similar operational needs in both civil security and defence sectors;
2. Technology level;
3. Market attractiveness;
4. Existing joint R&D.

Then, experts were asked to score each functional areas across four criteria in a systematic way. The results of the expert assessment yielded two areas with the largest potential for spin-offs: cyber security and sensor systems. Given the fact that cyber security and C3 are closely interlinked the results of two approaches are quite similar, and this provides an additional degree of confidence in the results. At the same time, the report suggest that the development of comprehensive technology roadmaps for the civil security domain and their comparison with the defence technology roadmap would provide a more systematic, comprehensive and detailed way to identify major areas for synergies.

3.6 Economic models

One particular element of this study is to identify economic models, that are used by industry to identify possible areas of interest for civil-military spin-offs/spin-ins". This part of the study identifies the factors that industry takes into account when assessing the potential for technologies to result in spin-offs from one sector of application (military, security or civilian) to another sector of application. It also examines the influence that the outcome of such an assessment may have on firms' behaviour with regard to technology development activities (i.e. the extent and form of firms' investments in research and technology development).

3.7 Policy options and Impact Assessment

The Commission has requested to study four main policy options for enhancing civil-military synergies and provide their impact assessment:

1. More systematic coordination of research activities between FP7 and EDA through the European Framework Cooperation;
2. Improved upstream coordination at the level of capability development through high-level stakeholder group;
3. Downstream coordination via development and use of 'hybrid' standards;
4. Use of Article 185 TFEU36 to support joint research effort.

After a discussion of these options in Chapter 6, Chapter 7 provides the impact assessment of these options. This assessment was done mostly on a qualitative basis using expert judgement. Chapter 7 also presents a quantitative assessment for some selected technologies and functional areas to illustrate a potential future state where civil-military synergies have reached an optimum scope.

3.8 Conclusions and recommendations

Finally, Chapter 8 presents the main conclusions and recommendations. First, a summary of observations on the current state of the defence and civil security synergies is given, followed by opportunities and recommendations for (increased) future synergies. Main findings of the policy options analysis and impact assessment conclude this Chapter.

[36] Article 185 TFEU states: "In implementing the multiannual framework programme, the Union may make provision, in agreement with the Member States concerned, for participation in research and development programmes undertaken by several Member States, including participation in the structures created for the execution of those programmes."

4 Case studies

4.1 Introduction

This Chapter presents an analysis of the military - civil security spin-off cases. The first section of the Chapter gives a broad overview of cases identified through systematic search. Its aim is to provide a broad scan of spin-off activity between the military and civil security sectors in the last decade or so. The spin-off examples in this section cover various functional areas of the defence and civil security industries, various stages of commercial development – from R&D to very successful commercial products, different technology levels and national markets.

In the second section of this Chapter, we selected some ten cases for a detailed analysis. This selection reflects the distribution of cases found in the broad scan and accessibility of information. By providing an in-depth description of the spin-off process, we identified the main factors affecting the success of spin-offs between the two sectors.

In a final section, we use the information acquired in the in-depth case studies for a discussion on barriers, success factors and more general characteristics of the spin-off process. These lessons learned serve as input for further Chapters in the report.

For this chapter we employ the case study methodology, i.e. "analysis of an individual unit (e.g., a person, group, or event) stressing developmental factors in relation to context"[37]. Since there is no statistical data on the spin-off activity this is the main method to analyse context and particular factors that determine outcome of the spin-off process. This method is widely used in social sciences, where more quantitative approaches face similar difficulties. While it might be difficult to draw general conclusions from an individual case, a broad selection of cases should improve validity of such conclusions.

4.2 Broad scan

This section provides an overview of the recent spin-off cases in the civil security and military markets. It contains cases from each of the nine functional areas (see paragraph 2.2) and for all three technology levels. As said earlier, we have primarily looked at "European" cases, in particular from the German, French, Swedish, and Dutch industries, but we have included non-EU examples, primarily from the US, as the American military and civil security market is the largest in the world. At the same time, national barriers matter only to a certain extent – a point that will be further illustrated in the next two sections. The list presented in this section could no doubt be further expanded with other cases. However, we feel confident that the overview of cases presented here is illustrative and representative for the dynamics and issues associated with military-civil security spin-offs.

Table 3.1 below provides a condensed overview of the spin-off cases we have identified. The table shows that the identified spin-off cases cover all functional area and technology levels. All cases are presented in table 3.2.They were identified through the expert knowledge of the project

[37] Flyvbjerg B., "Case Study," in N. Denzin and Y. Lincoln, eds., The Sage Handbook of Qualitative Research, 4th Edition (Thousand Oaks, CA: Sage), 2011, pp. 301-316.

participants and their institutions. In addition, we performed a literature review to expand our initial selection of cases.

For each spin-off case, a brief description is provided. Additionally, the table lists the functional area and technology level(s) at which the spin-off occurred, the spin-off direction (i.e. from security to military or the other way around) and the stage of commercialisation (i.e. R&D, pre-commercial or commercial). Some spin-off examples involve several technology levels. For example the *Iris scan system* case is classified under sensors as both sub-system and integrated system level. Other cases score at multiple functional areas. The case of *neutron tubes* was scored at both sensor level and CBRNE protection.

The section concludes with three charts that visually summarise the overall distribution of these cases per functional area, technology level and spin-off direction.

Table 4-1 Overview of spin-off case studies

Functional area	Technology level		
	Technology	Sub-system	Integrated System
Sensor systems and (sensor) information processing			
Command, Control and (Secure) Communications			
Training & Simulation			
CBRNE protection			
Physical security protection			
Protective clothing			
Cyber protection			
Non / less lethal weapons			
Platform integration and networked capabilities			

Table 4-2 List of spin-off cases

Case description	Functional area	Technology level	Sec◄►Mil	Stage
Wireless sensor networks Sownet Technologies (NL) provides distributed small disposable sensor networks for area surveillance. For example, a group of low-cost sensors can be spread over a field for the detection of persons or other movement.	Sensors	Sub-system	Mil►Sec	Commercial
POS This experimental program concerns the development of a robust position support system in buildings for the Netherlands Defence Force by a Dutch consortium. GPS does not provide position information in buildings, which is important for coordinated operations of a unit in order to prevent blue-on-blue force incidents. Spin-off to the civil security sector is envisaged (for use by, e.g. SWAT teams).	Sensors	Technology	Mil►Sec	R&D
Handheld Radars for Looking through Walls Cinside (SE) is a company developing easy-to-use handheld radar devices for the detection of movements through walls using Doppler radar. The device is currently being tested by defence forces. Similar devices are developed by other companies (e.g. the UK company Cambridge). Future sales for law enforcement purposes are projected.	Sensors	Sub-system	Sec►Mil	Pre-Commercial
Integrated Anti-Swimmer System An underwater surveillance system technology for detecting, tracking, classifying, localizing and notifying underwater threats. The system was developed by Kongsberg (NO), based on a military sonar. The spin-off was developed for the U.S. Coast Guard as an element of its Underwater Port Security System.	Sensors & Integration	Sub-system, integrated system	Mil►Sec	Commercial
Infrared camera's *(in-depth case description)* FLIR ATS (FR/US) manufactures thermal imaging cameras based on infrared detection. These cameras provide a picture of the outside world without any type of illumination (e.g. at night, or in a smoke-filled environment). FLIR sells both cooled and uncooled cameras. The latter have low performance but also low cost, volume and weight, and have been heavily used for security purposes. Cooled IR cameras have higher performance, longer range, but higher cost, larger volume and weight. These cameras too are increasingly used in the civil security market for tasks such as border control.	Sensors	Sub-system	Mil►Sec	Commercial
Squire A man-portable medium-range ground surveillance radar developed by Thales (FR) that can detect and classify moving targets on, or close to, the ground. Thales sold several adapted versions of the Squire called the Seeker, for security surveillance at oil platforms.	Sensors	Sub-system	Mil►Sec	Commercial

Case description	Functional area	Technology level	Sec◄►Mil	Stage
VarioView Handheld thermal imager, high resolution infrared detector with laser rangefinder. Developed by Jenoptics (DE), first for military use and later for border guards, customs and police.	Sensors	Sub-system	Mil►Sec	Commercial
Iris Scan Technology *(in depth case description)* Development of this technology by Iridian Technologies (US) and SAFRAN (FR) was funded by the US Defence Nuclear Agency. Iris recognition is the process of recognizing a person by analysing the random pattern of his or her iris. Its high effectiveness and low cost ensured its rapid adoption in military and later civil security markets.	Sensors	Sub-system	Mil►Sec	Commercial
SonarBell SonarBell is passive underwater acoustic device (sonar reflector) which works in conjunction with sonar to provide a clear echo return capable of locating underwater targets. It can be used to mark mines and underwater safe passages, to assist special forces with recovery of equipment and underwater navigation. Subsea Asset Location Technologies Limited (SALT Ltd) is a spin-off company from the UK Ministry of Defence's DSTL which was formed to make this military derived technology available to a wider market. SALT Ltd has designed a number of systems for military and security use based on passive SonarBell technology.	Sensor	Technology	Mil►Sec	Commercial
Dismounted Soldier System Soldier Modernisation Programs for the Royal Netherlands Army have led a Dutch consortium of TNO DO and other companies to the development of "smart vests", i.e. a fully combat-configured integrated soldier system. These vests include protective materials, connect devices, drink water systems and have space for soldier-based C3 systems that provide battlefield information. The consortium is developing a similar suit for firemen with "on scene information" of an incident.	Physical protection & Integration & C3	Integrated system	Mil►Sec	R&D
Geo profiling Geo profiling by e.g. Palantir (US) is a technique based on GIS (Geo Information Systems) to create maps of incidents in a certain area. In The Netherlands the application has first been used by the national police for making maps of crime in different neighbourhoods. In a later stage it has also been applied in military missions in for example Afghanistan.	C3	Technology	Sec►Mil	Commercial

Case description	Functional area	Technology level	Sec◄►Mil	Stage
Software Defined Radio Saab TransponderTech (SE) is launching the world's first fifth generation AIS (Automatic Identification Systems) using all-COTS hardware. The basic function of Automatic Identification Systems (AIS) is collision avoidance. The technology can be described as Software Defined Radio (SDR), building on 4G mobile communication hardware technology. It will be able to cover maritime and air traffic channels and the technology is used in both defence and civil security markets.	C3	Integrated system	Mil►Sec	Commercial
MOOVE A blue force tracking application developed by Thales (FR) for improving C3 for civil security actors (e.g. police). The application can be used on smart phones. During the process, several military actors showed interest in the application, which resulted in tests and trials.	C3	Integrated system	Sec►Mil	Pre-commercial
REMUS 100 A UUV used for mine counter measures. It was developed by the US Navy and Hydroid (a US company, currently owned by Kongsberg (NO)) for locating sea mines in mine counter measures in shallow waters. Later, the UUVs were purchased for civil security purposes (e.g. anti-terrorist measures, harbour protection).	C3 & sensors & integration	Integrated system	Mil►Sec	Commercial
SeaOtter UUV UUV system developed by Atlas Elektronik (DE) for mine detection and counter measures, covert intelligence, surveillance and rapid environmental assessment, sea bed mapping, hydrographical surveys. Originally of civil origin (system concept), it was later customized to military needs (payload).	C3 & integration	Integrated system	Sec►Mil	Commercial
AirRobot UAV AirRobot is a Vertical Takeoff and Landing (VTOL) Micro-UAV system that is based on a concept of civil origin developed by AirRobot (DE). It was later customized to military needs (i.e. payload) for military use (observation, reconnaissance, inspection).	C3 & integration	Integrated system	Sec►Mil	Commercial
LUNA UAV *(in-depth case description)* Real time surveillance UAV based on COTS technology and developed for military (all-weather, high-performance, modular payload). The producing company EMT Ingenieurgesellschaft (DE) currently tries to sell the technology on the civil (security) market.	C3 & integration	Integrated system	Mil►Sec	Pre-commercial
Rapid 3-D terrain mapping *(in-depth case description)* SAAB (SE) has developed a Navigation Demonstration Pod for C3 and rapid 3-D terrain mapping. This pod allows for terrain mapping from an aerial platform, using an array of sensors based upon COTS technology. In order to explore the potential of 3D maps for civil markets SAAB established a joint venture, which was later sold on.	C3 & Training & simulation	Sub- system, integrated system	Mil►Sec	Pre-commercial

Case description	Functional area	Technology level	Sec◄►Mil	Stage
Mayor game In the past years modelling and simulation has evolved into gaming, which has led to the development of context bases 'serious games' by Thales (FR) and TNO DO (NL). These serious games include NATO experiments on CDAG (Concept Development & Assessment Games), which are used to train strategic decision-making skills. In analogy with these games, public security management games have been developed for mayors and municipal authorities to emulate and train crisis management decision-making processes.	Training & simulation	Integrated system	Mil►Sec	Pre-Commercial
Threat Containment Unit Designed to safely transport a suspected explosive package away from an airport terminal with minimal disruption. The technology consists of layers of high impact steel, various composite material, blast suppressant chemicals or specialized fabrics that ensure high blast resistance or blast suppression. Originally developed by the US Navy for airport security. Now used by various military and civil security actors and developed by several, mostly US companies such as Aigis.	CBRNE	Sub-system	Mil►Sec	Commercial
Saratoga Blücher (DE) produces air permeable CBRN protective material. The company initially focused on protective clothing for civil and civil security purposes. As market demands and public funding priorities changed, Blücher started to focus on chemical and biological protective clothing, primarily for warfare protection and thus for the military market.	CBRNE & protective clothing	Technology	Sec►Mil	Commercial
J-FIRE The Joint Firefighter Integrated Response Ensemble (J-FIRE) is a protective lightweight over-garment that offers protection to fire and chemical hazards for fire-fighters, while not limiting their movement during operation. The gear was developed by the US Air Force and Army, based on a similar system used in the army. Now it is being developed by different companies worldwide (e.g. Blücher (DE) and Fire-Dex (US)).	Protective clothing	Technology	Mil►Sec	Commercial
Defender M *(in-depth case description)* TenCate (NL) developed an inherently heat- and flame resistant fabric called the Defender M for use in military uniforms. Later it was used in the production of uniforms for civil security actors such as riot police and SWAT-teams.	Protective clothing	Technology	Mil►Sec	Commercial

Case description	Functional area	Technology level	Sec◄►Mil	Stage
Pulse Plasma Coating P2i Ltd is a British company that developed unique liquid-repellent nano-coating technology. P2i originated as a project within the UK Government's Defence Science & Technology Laboratory (DSTL), to make soldiers' protective clothing more effective against chemical attack while maintaining comfort. In 2004 the company became the first DSTL Technology Transfer company, created to commercialize defence technologies developed by the UK Government. Nano-coating technology delivers high performance protection against oil and hazardous liquids for tactical clothing operating in the military and civil security domains.	Protective clothing	Technology	Mil►Sec	Commercial
Anti-MANPADS *(in-depth case description)* Anti man portable air defence systems (MANPADS) are technologies developed by several companies such as ELBIT Systems (IL), SAAB (SE) and Northrop Grumman Group (US) for protecting aircraft against guided missile attacks. After being in use for over 3 decades on military planes, these companies developed and sold similar technologies for the protection of civil aircraft.	Physical protection	Sub-system	Mil►Sec	Commercial
IRIS *(in-depth case description)* The Gatekeeper was developed by Thales (FR) in 2007 for littoral surveillance on ships used in, for example, anti-piracy missions. The system consists of a 360° panoramic surveillance and alerting system based on IR/ TV technology and helps in detecting small objects on the surface. IRIS is a smaller, lighter version of the Gatekeeper system, developed for the civil security market.	Physical protection & Sensors	Integrated system	Mil►Sec	Pre-Commercial
Integrated head unit Within the Dutch Soldier Modernization Programme, a development project exists for the concept of Integrated head protection for mostly Army units. A Dutch consortium is looking into similar products that could be used for civil security actors.	Physical protection	Sub-system	Mil►Sec	R&D
FOX-IT Data Diode *(in-depth case description)* The FOX-IT and Brightside (NL) data diode consists of a hardware part supported by specially developed software, which makes it possible to transfer information from a lower security information environment to higher security environments. It was developed for securing data transfer of governments. An adapted version of the Data diode is now also used for civil security protection, such as public critical infrastructure protection. This version of the data diode is designed to allow operators to securely receive information to monitor processes of critical infrastructures.	Cyber protection	Sub-system	Mil►Sec	Commercial

Case description	Functional area	Technology level	Sec◄►Mil	Stage
Cassadian - cyber security Cassadian (DE) provides consultancy services in the field of cyber security, including concept generation, risk management, technology awareness along with regulatory aspects. Initial focus was on the defence sector, now the company is also providing services to the civil (security) sector.	Cyber protection	Integrated system	Mil►Sec	Commercial
Taser *(in-depth case description)* Taser is an electroshock weapon that was developed by Taser International (US) and causes strong muscle contractions. After it was used on a large scale by (US) law enforcement agencies, a more powerful version found application for use by military forces engaged in stability operations.	Non-lethal weapons	Sub-system	Sec►Mil	Commercial
SODERN Neutron tubes *(in-depth case description)* SODERN (FR) developed neutron tubes for the French nuclear weapon programme. In recent years the technology has been used in new application for detection on dangerous or illicit substances (e.g. for airport security) and demining. Safety concerns however have so far hampered sales in the security market.	CBRNE & Sensors	Technology and sub-system	Mil►Sec	Pre-Commercial
Eurocopter EC145 EC 145 is a twin-engine light utility helicopter manufactured by Eurocopter, a division of EADS. It is used for civil (including security) applications. The UH-72 Lacota is a militarized version of the Eurocopter EC145, built by American Eurocopter division of EADS North America for the US Army. Adaptations to the aircraft included a secure military radio and an additional ventilation system, among other.	Integration	Integrated system	Civil (Sec) ►Mil	Commercial

The following charts show the resulting distribution of the cases from this broad scan. As chart 3.1 illustrates, we have found cases for all nine functional areas, and where two areas, “Sensors” and “Command, Control and Communications” (C3), show more spin-off examples than the other ones. Chart 3.2 shows that spin-off activity at integrated system and sub-system level occurs substantially more than at the level of technologies and components. Finally, the spin-off direction chart (Chart 3.3) indicates that spin-off from military to civil security is much higher than the other way around. These results will be discussed in more detail in the final section of this Chapter.

Chart 4.1 Cases per functional area

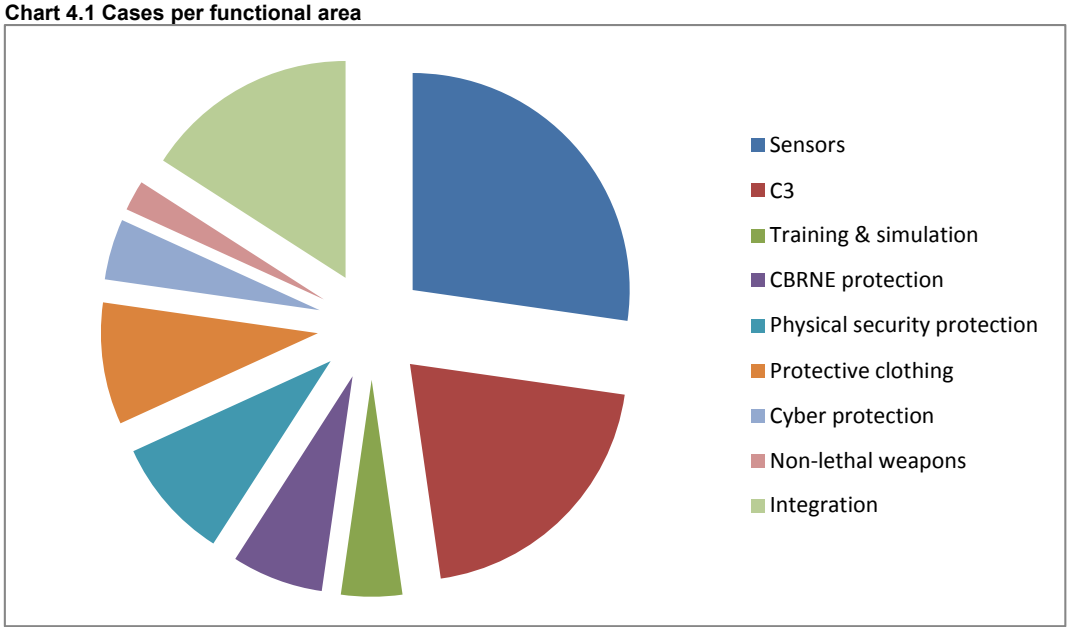


Chart 4.2 Cases per technology level

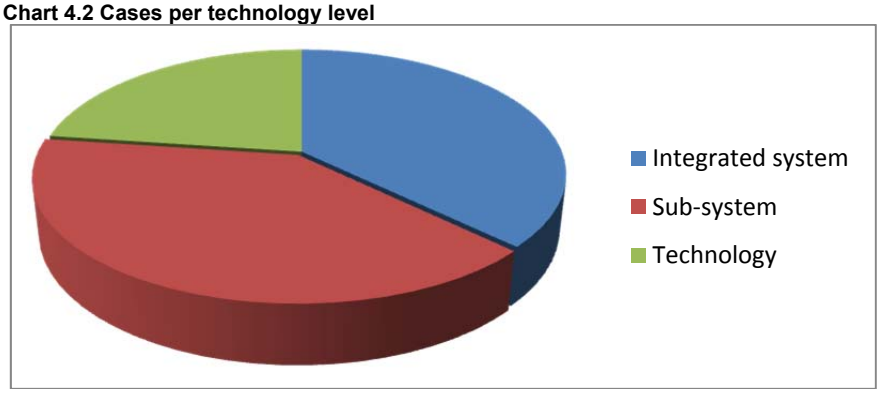
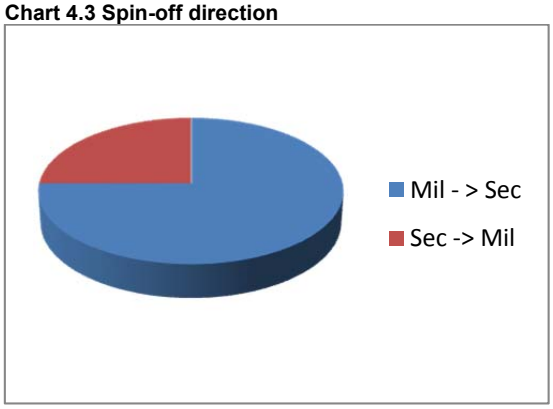


Chart 4.3 Spin-off direction



4.3 In-depth case studies

From the broad scan, a number of cases has been selected for in-depth analysis. Criteria for selection included data availability, coverage of the respective functional areas and stage of commercial readiness. Furthermore, the selection was driven by assumed market size (potential or actual). This resulted in the selection of ten cases. From these in-depth case studies we intend to understand innovation dynamics, barriers and success factors that have an impact on the spin-off process. Information was gathered by conducting interviews with company representatives, and supported by an extensive literature review of used technologies and, where possible, the spin-off process.

Table 3.3 below presents a schematic overview of the selected cases in terms of technology level and functional area. The numbers in the cells correspond to the case numbers in this section.

Each of the ten in-depth case studies includes a description of the technology, its initial area of use, how it was adapted and eventually found (or is finding) its way to the spin-off market. Where possible, data has been included to indicate market size and potential. Special attention has been paid to factors that facilitate or inhibit spin-off process, and are described in the conclusions. Some cases concern specific technologies primarily developed by one company, for example the Defender M, fire resistant fabrics developed by Tencate or the Taser stungun developed by Taser. Other case descriptions are more generic in nature, i.e. where a number of companies produce a similar product. In those cases, we not only focussed on a specific technology and company, but also on the wider spin-off trends (e.g. the LUNA UAV case study).

Table 4-3 Overview of in-depth spin-off case studies

Functional area	Technology level		
	Technology	Sub-system	Integrated system
Sensor systems and (sensor) information processing		2;4	1
Command, Control and (Secure) Communications		5;9	3;5
Training & Simulation			5
CBRNE protection	1	1	
Physical security protection		6	3
Protective clothing	7		
Cyber protection		10	
Non / less lethal weapons		8	
Platform integration and networked capabilities		9	
Total	***2***	***9***	***5***

4.3.1 *Case 1: Neutron tubes/ SODERN [CBRNE][38]*

Technology

Neutron tubes serve as a source of a neutron flux. Atoms, when exposed to a neutron radiation, respond by emitting γ (gamma) rays. Because different elements respond differently, it becomes possible to determine the elements of the exposed object and their concentration. This opens an opportunity to use the technology in a detection system.

Original use of the technology: defence

The underlying technology was first developed for military purposes as a neutron initiator for fission chain reaction in nuclear weapons. The origins are closely related to the know-how in the vacuum tube field developed by Philips. The Dutch company had a number of subsidiaries in France, and some of these developed products for the military use (radar wave tubes, neutron tubes, image intensifier tubes).

When France embarked on the nuclear weapon programme, this know-how was used by the SODERN[39] subsidiary (created by Philips in 1962) to design neutron tubes for nuclear weapons. The French company SODERN is currently owned by EADS Astrium (90%) and CEA (10%) and employs 340 people with turnover of € 59 million. 35% of turnover is spent on R&D.

New area of application: civil security

After initial military use of neutron tubes, SODERN started to develop new civil applications for them, for example, for non-destructive materials control, ore and bulk material control, and security purposes. The use of the technology in civil security is relatively recent. Its main applications in the security domain include detection of illicit or dangerous materials (explosives, drugs, dangerous chemical substances, fissile materials) in baggage, vehicles or containers (land or marine) and search for buried or hidden explosives and treatment of historic munitions).

The security use of neutron tubes accounts for approximately 5% of SODERN's turnover (i.e. €3 million); the other non-military uses of neutron tubes represent another 10% of the total turnover (i.e. €6 million). In 2010 SODERN concluded a strategic alliance with the Dutch company PANalytical (that originated in the Philips group). This alliance is based on the complementarities of SODERN's neutron technology and PANalytical's X ray technology, and enables SODERN's customers to benefit from PANalytical's worldwide network.[40]

SODERN's strategy has been aimed at extending its basic know-how to non military applications. In 1990s, the first demonstrator of a SODERN explosives detector was tested at the Los Angeles airport.[41] Today neutron tube production for civil applications is already significantly greater than for military use, and this trend will strengthen in the future. Industrial applications of SODERN's neutron tubes in the oil industry, the mining and cement markets are already well developed.

Neutron analysis technology offers significant benefits in the civil security field as well. It can detect dangerous or illicit (drugs) materials, such as various explosives (semtex, TNT, C4), drugs and radiologic and nuclear materials. However, there are significant differences in applications of neutron tubes in the military and civil (including civil security) fields. Military applications use high neutron flux with a long life span when not in-use and high reliability. Civilian applications use lower neutron flux and have a long usage time. Even more important is the integration of neutron tubes

---

38 Most information used in this case description was gathered through interviews with people from SODERN.

39 www.sodern.com.

40 http://www.sodern.com/sites/en/ref/News_110.html.

41 http://www.sodern.com/sites/en/ref/Key-Milestones_44.html.

with other elements (gamma detectors, electronics) into the system that would meet demanding requirement of civilian users in terms of size, safety, reliability, accuracy, etc. Other challenges in the spin-off process were to increase the life time of neutron tubes and to reduce their cost. SODERN plans to increase the life-time from the current 15 000 hours to 30 000 or even 50 000 hours. This will help to expand applications and market for neutron tubes. Another objective was to reduce the cost of the analyser, and in particular the gamma ray detector (crystals).

In the security field applications of neutron analysis has been demonstrated especially for detection of improvised explosive devices (for example, in unattended luggage, at check points), for chemical weapon identification. However, application of this technology for air transport security faces several difficulties:

- *technical:* very small quantities of explosives must be detected. National Research Council in the U.S. in its 2002 assessment of the pulse fast neutron analysis technology for explosive detection in air cargo containers came to the conclusion that it was not yet ready for airport testing [42];
- *economic and organisational:* it may be more economic if in doubt to destroy a piece of baggage (even if this may involve a risk of dispersal of chemical agents);
- *regulatory:* in France regulation prohibits irradiation of a piece of baggage as that may activate the food products, jewellery, toys or cosmetics it may contain. Experience has shown, however, that the residual activity remaining after inspection is not high enough to be measured after a few minutes.

These difficulties are not necessarily insurmountable in the long term. If the advantages to society are proven, the public authorities may consider revising current regulation. In the short term however, this is a barrier to application in the field of airport security.

A facilitating factor is that SODERN neutron sources are ON/OFF sources, which provides a relatively high degree of safety in their use. The restriction area is quite small (about 10 metres around the source) and can be accessed at once after the source has been turned off.

Still, use of neutron tubes for several applications in the security domain requires substantial R&D to develop demonstrators that can open the market, and to acquire know-how in the use of such systems. So far, SODERN is only beginning to sell demonstrators and applications in the security field and use of neutron tubes in the security markets, especially for demining (military and civil security) is in the take-off phase.

Conclusion

The case of SODERN illustrates the complex, and in this particular case, spiral, character and nature of spin-offs. The neutron tube technology was developed for military purposes but it was based on civil technology. Then it found new applications in the civil sector, when SODERN started marketing neutron tubes for the mining and cement industries (in the 1980s). Only recently the technology began to be used in the field of civil security. Interestingly, these civil security applications gave birth to new military applications (demining).

The case also demonstrates an important role of regulation. Currently French regulation prohibits its use for baggage control on the bases of health concerns. This acts as a strong barrier to the use of the neutron technology for baggage screening in airports.

---

[42] http://www.nap.edu/openbook.php?record_id=10428&page=1.

4.3.2 *Case 2: Infrared Cameras [sensor systems and (sensor) information processing]*[43]

Technology

An infrared (IR) camera is basically composed of 3 sub-systems: an IR detector, an optical system and electronics (both hardware and software). The detector is the key element of an infrared camera driving its cost and performance. Two major product categories are distinguished by the type of IR sensors used. Cooled sensors/cameras have higher performance, longer range, but higher cost, larger volume and weight. On the other hand, uncooled sensors/cameras have lower performance and a lower range, but lower cost, volume and weight.

FLIR ATS (Advanced Thermal Solutions) is a French SME specialising in the design and manufacturing of high performance thermal imaging cameras based on infrared detection. Thermal imaging cameras can obtain a completely passive picture of the outside world based on thermal emissions only and require no external light or thermal source such as the sun, moon or infrared illuminator.

Original use of the technology: defence

Both types of IR sensors have been developed by the military although they now follow a different path. The uncooled sensor cameras are now mostly used in the civil field, and this technology is fully driven by civilian applications and private investment, unlike the cooled technology that remains defence driven. The French company FLIR ATS produces thermal imaging sensors and sells these mostly to civil markets, with security accounting for approximately 40% of the turnover. It has a revenue of approximately €10 million and about 100 employees. Previously known as CEDIP (founded in 1989) in 2008 the company became a subsidiary of FLIR Systems (US). FLIR systems is the world leader in thermal imaging and sells products to both military and civil customers representing respectively 40% and 60% of the group activity (security accounting approximately for 15 to 20%).

In general, the relative market size for cooled and uncooled sensors is in a ratio of 1 to 100 in terms of units, with less than a thousand cooled cameras sold per year, and hundreds of thousand of uncooled cameras. The overall market for both technologies is 60% for the military, 13% security and 27% professional. Main manufacturers of sensors include SOFRADIR-ULIS (France), Selex (Italy), SCD (Israel), FLIR (US), etc. Defence suppliers who are heavily involved in the ownership structure of cooled sensors manufacturers include SOFRADIR (Thales-Safran), Selex (Finmeccanica) and SCD (Elbit, Rafael). Both thermal imaging sensors and cameras are classified technologies that must comply with stringent export control regulations, particularly for cooled sensors and cameras (dual use regulations in Europe, ITAR regulations in the US).

New areas of application: civil security

High-performance cooled sensor cameras are still mainly used by the military. Some more specialised civil applications include border security or highly critical infrastructure, where longer range and higher performance are essential. Other civil applications for cooled cameras include scientific research and industrial process control. Uncooled cameras are much more used in the security field. Applications include critical infrastructure protection, airport security and standard surveillance.

[43] This case description is to a large extend based on interviews with FLIR ATS staff.

Whereas the military market is still proportionally large, it is much less of a driver for growth and developing new products. Therefore companies need to diversify their market base and identify new growth drivers in civil applications as demonstrated by uncooled sensors/cameras spin-off from the military to the civil domain. The share of the military segment is decreasing, particularly in the uncooled segment, where new markets, in particular in the automotive market, are booming (for example, 500,000 units are expected to be sold by 2016).

Larger civil markets volumes enabled unprecedented optimization of uncooled detectors and cameras in terms of volume, performance, robustness and cost, which in turn benefited military clients. A similar move for cooled sensor technologies to the civil domain would likely bring comparable benefits. A cooled camera remains up to 20 times more expensive than an uncooled camera, essentially due to the detector technology. If cooled sensor prices could be cut, it is expected that considerable further expansion of the market could come through. FLIR Systems projects that with the proper investment in R&D, sensor prices would be reduced significantly, and that this would enable a tenfold increase in the market.

FLIR Systems has 2 separate and dedicated divisions respectively for government (military) and commercial systems (civil). This has to do with the different demands of customers from both markets. Military customers look for specific performances with programme-based technological development as opposed to civil markets, where suppliers develop/propose standard products based on their own understanding of the market requirements. Therefore, selling to both military and civil markets will require a dedicated approach and strategies from a supplier perspective.

Conclusion

This case shows two major barriers and one facilitating factor for spin-off. First, some regulatory issues may limit spin-off potential. Specifically, export licensing is a complex process to go through which significantly increases time to market and adds to product cost. In addition the lack of predictability, visibility on both the approach and the criteria used by public authorities is limiting the development of the civil market. The process is very similar to the way data protection authorities work and with the same drawbacks (lack of clarity in the assessment criteria, lack of coordination between Member States, lengthy and costly processes). This barrier is particularly severe for cooled sensors and cameras.

A second barrier is the high unit costs for cooled cameras that render the products too expensive for civil markets. Uncooled sensors have strongly benefited from commercial investment in optimization of the technology and its mass production. It is possible to similarly decrease unit costs of cooled cameras by investments in technology optimization and manufacturing. However, such investment carries large risks, since they may not be justified by the increased demand caused by lower prices. Governments could reduce these risks by, for example, simplifying procedures and regulations to facilitate export market development.

4.3.3 Case 3: IRIS [physical protection/C3][44]

Technology

The IRIS is a smaller, simplified version of the Gatekeeper system, a 360° panoramic surveillance and alerting system based on TV and infrared technology. The Gatekeeper was developed by Thales in 2007 for littoral surveillance on warships. The system helps in detecting small objects on

[44] Since the product discussed is in pre-commercial state, most information came from interviews with Thales.

the surface. The IRIS is a similar device, but without the use of TV HD camera's and a less sophisticated sensor head.

Original use of the technology: defence

The Gatekeeper has been developed by Thales for addressing asymmetric warfare threats and improving situational awareness of naval ships. This passive surveillance system is built with non-rotating infrared and TV cameras that provide a continuous 360° panoramic visual overview of the ship's environment. Tracking facilities are provided to track small surface targets.[45] Unlike traditional infrared search and track, which mechanically scan the surroundings, the Gatekeeper utilizes multiple static sensor heads incorporating large infrared focal plane arrays, an advanced optical design and dedicated processing algorithms on COTS processing hardware to provide enhanced ship self-protection, particularly in the littoral environment.

The first order was received from the Royal Netherlands Navy to equip four new patrol ships ordered in December 2010. Thales has sold around 10 Gatekeeper systems. Total market size is hard to establish. Visiongain has estimated that the value of the global electro optical infrared systems market in 2011 would reach $7.47 billion.[46]

New area of application: civil security

From 2007 onwards, several trials have been held in harbour environments to test the Gatekeepers' use in civil security environments for automatic target detection with infrared cameras. In 2010 and 2011 further trials successfully illustrated the potential of the technology for the civil security and justified additional R&D expenditure to develop a less costly version of the Gatekeeper.. Since the security market has different, often less stringent demands than the military markets, Thales was able to substantially reduce the cost of the device, while retaining almost the same functionality as the Gatekeeper. This process resulted in the IRIS system. Costs were cut by reducing some high quality features: the IRIS system lacks the use of high quality cameras and has a less sophisticated sensor head. With these adaptations, the final price of the device will be significantly lower than that of the Gatekeeper.

The development of the IRIS was mostly driven by the desire to develop a "lighter" version of the Gatekeeper which could bear interest from other markets. According to Thales, the development of the IRIS fits in a more general evolution of demand for security surveillance. At first, companies or governments react to security concerns mostly by focusing on the low hanging fruit: purchasing (more) camera's and/or hiring security personnel. But once people have been hired and camera's have been purchased, it becomes much more useful to invest in clever ways to integrate information that these camera's or other technologies provide. Thales' focus on developing the IRIS anticipates this changing need.

Thales sees several spin-off domains, ranging from the oil and gas industry to merchant vessels (e.g. anti-piracy measures), luxury yachts and large scale event security. Other companies delivering similar products are Kongsberg Maritime (NO), Axsys technologies (US) and Cloud Cap Technologies (US).

As the IRIS System has not been introduced formally yet, market development and market introduction is in its infancy.

Conclusion

---

45 http://www.thalesgroup.com/gatekeeper/.

46 http://www.visiongain.com/Report/704/The-Military-Electro-Optical-Infrared-%28EO-IR%29-Systems-Market-2011-2021.

This case illustrates that along with product development entering a new market requires significant efforts (entry costs) to understand market conditions, (performance) requirements as well as pricing strategies. In addition, the development of the IRIS also shows that technology demands in the military market are often much higher than in the security domain. By replacing some costly parts of the system with cheaper substitutes with a similar functionality, the price could be lowered to a tenth of that of the Gatekeeper. And finally, as a spokesman at Thales pointed out, what may make the sale of the IRIS most difficult is that it hasn't been sold yet.

4.3.4 Case 4: Iris Scan Technology [sensor systems and (sensor) information processing]

Technology

Biometric technology is an automated method of recognizing an individual based on measurable, biological and behavioural characteristics. The most common biometric technologies are fingerprint, face, iris, voice, signature and hand geometry. This case focuses on the iris recognition, which is the process of recognizing a person by analysing the random pattern of his or her iris.

Due to randomness in irises, it is very difficult to forge or imitate the iris of an individual. Besides this physiological benefit, iris scan technology is not as intrusive as for example fingerprints, because there is no direct contact between the individual and the camera. The accuracy of the scanning technology is another major benefit as well as the speed of the process.[47] Nevertheless, there are some disadvantages to the iris scan technology. Because the iris is a very small organ, scanning from a distance is difficult as well as scanning a moving target. In addition, the camera used to scan the iris needs to have the correct amount of illumination to capture an accurate image of the iris. While intrusiveness is minimal, there is still need for cooperation from an individual to enrol in the system and undergo the subsequent authentication scans.

Original use of the technology: defence

The first prototype iris scan device was developed for the U.S. Defense Nuclear Agency in 1995.[48] Within the U.S. Department of Defense there was a need to provide an entry/access control system that would be capable of identifying and verifying the identity of persons with a high degree of confidence and without a man in the loop. A study by the Defence Nuclear Agency (DNA) concluded that no existing system, technology or methodology could meet the objective. Of the systems and technologies under development, only the iris scan systems promised a positive identification and verification with a high degree of accuracy. The DNA awarded a research and development contract to further develop the iris scan technology. The iris-based proof-of-concept system that was built and designed under this contract met or exceeded all standards and operational performance requirements by DNA. Moreover, the estimated costs for the system were seen as reasonable and cost-effective, especially when compared to the performance and cost of other biometric access control systems available at that time.[49]

New area of application: civil security

While the iris scan was initially developed as an access/control mechanism, the first application of the technology in the civil security domain was to verify criminals and suspected criminals. In 1996, Lancaster County Prison in Pennsylvania became the first correctional facility to use iris scanning, because fingerprint test were more time consuming.[50]

---

47 http://www.sans.org/reading_room/whitepapers/authentication/iris-recognition-technology-improved-authentication_132.

48 It was renamed in 1996 to the "Defense Special Weapons Agency".

49 http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA302620.

50 http://articles.cnn.com/2000-07-19/tech/iris.scan.idg_1_scans-airport-today-jerry-orr?_s=PM:TECH.

Soon after, the military started to use iris scanning for similar purposes. During the 1999 conflict in the Balkans the iris scan technology was part of the Biometric Automated Toolkit (BAT), a system consisting of a laptop with identification processing software and peripheral devices including a hand-held iris scanner, digital camera, and fingerprint reader. The laptops connected to a series of servers to ensure regular updates of vital biometric records. The BAT was used to identify local nationals causing problems to U.S. installations who gained re-entry after being expelled somewhere else.[51] Currently iris scans are used in the operation Enduring Freedom and Iraqi Freedom – in a handheld device. In these missions the system provides a central, authoritative repository for biometric records. It catalogues biometric data (iris') taken from detainees, enemy combatants, and other persons of interest.

It was not until the 9/11 attacks that the technology became an acceptable application for civil security purposes. The terrorist attacks dramatically lowered the general public's resistance to technology previously viewed as invasive. Moreover, in the U.S., the Patriot Act, gave a legislative green light for the use of biometric technology. These developments accelerated penetration of the technology in the civil security domain. However, the use of biometrics remains sensitive to privacy concerns.

In 2005 the restrictive patent, covering the basic concept of the iris scan, expired opening opportunities for other companies to develop their own algorithms for iris recognition.[52] The patent on Dr. Daugman's algorithms technology have expired in 2011.[53]

Sales of iris scan devices have grown at the average rate of 18.8% between 2002 and 2007. By 2017 the iris scan technology is forecasted to have a 19% share of the global biometrics market, up from 8% in 2009. The revenue is expected to increase to $2.1 billion from $206.3 million, according to Acuity.

Since 2001 border control has become one the main users of the iris scan technology in the civil security domain. The United Arab Emirates, for example has been operating an expellee tracking system since 2001. All of the UAE's land, air and sea ports of entry are equipped with systems and all foreign nationals who enter the UAE are processed through iris camera's at immigration. In addition, several airports, such as Schiphol (Netherlands), Frankfurt (Germany) and Heathrow and Gatwick (United Kingdom) use the iris scan for border control.[54] Police forces and riot police forces have also shown an interest in the portable iris scan technology. The New York police has been using handheld iris scanners since November 2010 to identify prisoners and to ensure that suspects appearing before judges are not misidentified.[55] Iris scan is also used in the NEXUS, Canada-United States program for simplified border crossing between the two countries by pre-approved, low-risk travellers.[56].

The main producer of iris scanners is Iridian Technologies in the U.S. that developed a prototype for the DNA. L1 Identity Solutions, which was recently acquired by the French SAFRAN group developed the HIIDE, which is the most widely deployed multi-modal device with defence agencies. The U.S. DoD recently ordered ten million dollars worth of them. The HIIDE is used in Operation

---

51 http://asc.army.mil/docs/pubs/alt/2010/2_AprMayJun/articles/14_DOD_Biometrics--Lifting_the_Veil_of_Insurgent_Identity_201002.pdf.

52 http://www.biometrics.gov/Documents/irisrec.pdf.

53 http://www.bloomberg.com/news/2011-02-02/-minority-report-may-come-to-real-world-with-iris-recognition.html.

54 http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf and http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/.

55 http://online.wsj.com/article/SB10001424052748703326204575617031249438718.html.

56 http://www.cbsa-asfc.gc.ca/prog/nexus/enrol-inscrire-eng.html

Enduring Freedom and Operation Iraqi Freedom for counter insurgency purposes.[57] Alditech is a British company who produces the IrisGuard IG-AD100 and IrisGuard IG-H100 for border control, immigration and custom identification projects. [58]

Conclusion

Iris scanning technology is a recent development but its technological advantages helped it to spread rapidly. Since the need for identification is common to military and civil security the spin-off from the military to civil security domain was very quick and seamless. The technology did not require any significant adaptation for its spin-off. Its integration into hand-held devices was required by both military and civil security forces.

Expiration of the current patent might increase competition in this field and further boost the spread of the technology. One constraining factor, especially for some governments, was concern about privacy infringement and public reaction to it. Because of this, governments have been hesitant to broadly apply iris scanning technology in comparison to the private sector.

Another important point that the case illustrates is the importance of merger and acquisition activity for spin-offs and technology diffusion in general. One of the leading producers in this field, L1 Identity Solutions was recently acquired by SAFRAN Group. This might lead to increased use of iris scan technology in Europe as SAFRAN might use its marketing and sales capabilities here to expand sales of this technology.

4.3.5 Case 5: C3 Technologies and Rapid 3D Mapping – SAAB [C3/Training & Simulation][59]

Technology

The case deals with rapid three-dimensional terrain mapping from an aerial platform, using an array of sensors based upon COTS technology. In order to process the multi-sensor data into high-resolution, high-quality mapping products, advanced signal processing algorithms are required. In this area, SAAB could fall back upon its knowledge and expertise from the defence domain.

Original use of the technology: defence

In 2001 the Swedish Armed Forces (SWAF) launched a new strategy for technology and acquisition, emphasizing the need to explore the possibilities of “spin-ins” of civil technology into military applications through the use of COTS.[60] This strategy included an increased emphasis on demonstrators and evaluations of existing technologies to counterbalance the traditional focus on internal development projects and long-ranging contracts for defence materiel. In the case described here, COTS sensors were used in the Navigation Demonstration Pod, Navdemopod (2002-2006), which became the starting point of 3D-mapping as a military spin-off into a civil business success.[61] In this project, the challenge was to integrate these sensors with an advanced signal processing capability. The concept explicitly aimed for compensating for relatively low performance of inexpensive COTS components through high performance in signal and image processing, emphasizing the integration of different sensors. This gave new possibilities for flexibility, both in terms of modular design for an in-built scalability, but also in terms of ease of

---

57 http://www.gizmag.com/hiide-portable-biometric-device/15144/.

58 http://www.aditech.co.uk/IrisGuardH100.html.

59 Much of the information used in this case description was gathered through interviews with people from SAAB.

60 Bjurström, E and Brising, D. (2001) (Eds.) ”Strategi för Försvarsmaktens materielförsörjning”, [”Strategy for technology and acquisition of the Swedish Armed Forces”, in Swedish] Swedish Armed Forces, 2001, HKV 23 241:63210.

61 For more information on the technical details of 3D mapping, see http://144.206.159.178/FT/CONF/16414540/16414549.pdf.

adaption for different civil and military applications. SAAB's previous knowledge in image processing was crucial for this development.

The Navdemopod demonstrator consisted of a pod designed for aerial platforms (in particular future Unmanned Aerial Vehicles) with a great number of sensors generating reference data to determine exact positions and movements, as well as an extensive payload of sensors to be tested and evaluated. Radar and laser meters supplied the legacy terrain-navigation system Ternav with altitude data. A simple video camera was used to register the terrain in order to identify distortions of radar reflexes in vegetation or over waters. The integration of sensor data required extremely precise registration and time-stamping of all sensor and reference data. This required exploring new technologies within the area of micromechanical inertial navigation sensors – not only in laboratory environments, but in real-life aerial conditions.[62]

During the Navdemopod project period 2002-2006, the civil market for digital cameras exploded and its potential was further explored. Together with SAABs 20 year old but fast stereo-picture algorithms, affordable COTS digital cameras could be used to generate high resolution 3D pictures of the terrain. The results were stunning. At the same time, the increased capacity of the sensors provided new challenges: the greater detail the sensor has, the more clearly its deficiencies would expose themselves. While earlier knowledge and new civil technology provided the conditions, concrete and practical experience allowed for the functional mix of different methods and quite extensive "tricks and fixes" needed to come up with good results in the image processing.

As the Navdemopod project ended in 2006, many of the initial ambitions had been tested, but the feature that attained most attention was the newly identified potentials of 3D mapping in real time. The micromechanical inertial navigation sensors had been forecasted to become both inexpensive and more high-performing. However, present evidence demonstrates some degree of overoptimistic predictions of the past. High quality products, not least in terms of resistance to real-life exposure to temperature variations and vibrations, will still not be cheap, reflecting a weak demand on the market for components with military specification. However, application of COTS have shown to be a matter of trade-offs. In the case of the Navdemopod, the assumption that it would be possible to compensate for lower quality sensors by increasing ambitions on higher systems integration and processing levels was rewarded with results beyond expectations. SAAB was awarded a SEK 42 million contract from the Swedish Defence Material Administration (FMV), to supply SWAF with rapid 3D mapping capabilities for use in national as well as international operations.[63]

New areas of application: civil (security)

During the project, the conviction grew within the project group that image generating sensors would be used to a wider extent in future navigation systems, also allowing a closer integration between target seeker and navigation systems. A natural application in civil (security) markets would be in the field of training and simulation. However, the SWAF policy and strategy for technology and acquisition also played a crucial role in the relation between SAAB and FMV, which made clear the effect of the government's policy through FMV.

In the prolongation of the Navdemopod project, in order to explore the potential of 3D maps for civil markets SAAB established a joint venture with a Norwegian risk capital company, investing in the further development of the automatic generation of 3D maps for civil applications. The company C3

---

62 http://www.fmv.se/upload/Bilder%20och%20dokument/Publikationer/rapporter/16%20Navdemo.pdf.

63 http://www.saabgroup.com/en/about-saab/newsroom/press-releases--news/2010---7/saab-recives-order-from-fmv-regarding-3d-maps/.

Technologies was founded in 2008, with SAAB as main owner. In the following years, C3 Technologies attracted a massive interest in its revolutionary methods to generate three-dimensional geographical maps, automatically and within few hours after flying over an area their 3D maps. By the end of 2010 the company had 22 employees and focused on its international expansion. What was initially a side product of navigation now had become the main product, but with the distinguishing feature of an accuracy of measurement and 3D modelling down to 10 cm precision. Hence, the algorithms made for military navigation purposes showed to be a crucial feature of the commercial success. In July 2011, SAAB sold its 57.8 % share of its subsidiary company C3 Technologies for $150 Million, rendering a net profit of $135 Million.[64] The buyer remains unknown, but most analysts point at Apple.

While the technology showed success also in the civil market, the selling of C3 Technologies may indicate the challenges of reaching out to a completely different market than the one where the company normally operates. If the technology is so promising, one might ask why SAAB didn't realize that potential themselves. A realistic interpretation is that this should be seen as an indication of the difficulties for a defence company to operate in a completely different market. Hence, to reach a non-public civil market, defence companies would at least need a civil partner or a civil customer for the technology. Since SAAB has chosen to build its civil security concepts on network-centric solutions, characterized by modularity and thereby also upgradeability, the challenges are typically not a matter of technology, but of understanding the difference between the military and the civil security markets. The upgradeability of systems is an efficient means to allow for civilian actors to buy the high-level systems integration solutions first and wait and see about the needed performance of specific components, i.e. let time resolve remaining uncertainties in cost/performance trade-offs. However, what is emphasized more than anything else by the interviewees are the challenges in understanding different business cultures in terms of verbal conceptualization and the packaging of technologies and services in a way that appeals to the civil markets.

In order to become attractive for the civil security market, the technology needs some context to be understandable. As was underlined at SAAB, successful spin-off to civil markets necessitate a different approach with more emphasis on selling the product. In line with this, the rapid 3D mapping was presented and actively marketed as required for different areas, such as telecommunications, power distribution or traffic planning. The service was defined very broadly: actors as the Swedish Environmental Protection Agency need an overview of the general situation as much as the SWAF needs to keep track of their installations. Finding new applications of the technology is much a matter of reorientation, adapting to different kind of customer relations and the soft skills necessary to show and understand the customer. Another limiting factor in the search for civil security concepts is the difference in language and terminology.

Conclusion

The SAAB 3D mapping case has a number of characteristics which may make it interesting on a more general and principal level, beyond the specific case.

In principle, the combination of academic research and practical experience could have been achieved by civil companies as well. However, what made the developments at SAAB possible was that many of the components were already in place, not least thanks to decades of experience in navigation, systems integration, signal processing and, especially, stereo-image processing. Also, the access to real-life aerial tests were necessary and may have provided obstacles for companies

[64] http://www.saabgroup.com/About-Saab/Newsroom/Press-releases--News/2011---7/Saab-divest-its-shares-in-C3-Technologies/.

not operating in that area. Furthermore, many civilian companies wouldn't have had the reasons to build such deep expertise in relevant areas and may have had problems generating capital at early stages of the development, given the great amount of uncertainties and the serendipity of the process.

Related major challenge is one of balance between the more value for money and the military attitude of "it has to work". It has also to do with the maturity of the technology. In military markets, the task is often to "just solve the problem" at almost any cost, while in civil markets the customer will typically prefer to wait and see and complement their acquisition when the technology is mature enough and is more affordable. Scalability allows for such adaptation and hence becomes a key to success in civil markets. In addition, there is a legacy and an image talking against the success of defence companies in civil markets: technology with military background is typically met with suspicion of being too costly.

The challenges for further exploitation of dual uses of the technologies presented here, seem to lie in "soft" aspects of marketing and imagination, rather than in technological obstacles to new applications. This characteristic may be explained by the innovative part of the C3 mapping technologies lying in higher levels of systems integration, rather than in specific military technologies on the component level.

Another critical issue to be discussed based on this case, is how to achieve sufficiently deep and broad knowledge and experience to achieve successful systems integration also in smaller companies or in companies looking for new markets. It's an open question to which extent an increased staff moving between industry, university and customers can stimulate innovativeness and what the role of governmental or independent research institutes may be.

4.3.6 Case 6: Protection against MANPADS [Physical protection]

Technology

Portable surface to air missiles, also known as "man portable air defence systems" (MANPADS), are designed for use by individuals or small teams of soldiers against aircraft. The military developed Anti-MANPADS systems for protecting aircraft against these guided missile attacks. Originally, decoy/flare-dispensing systems were used to confuse a missile's heat-seeking sensors. More recently, directed infrared countermeasures systems have been developed that use sophisticated sensors and infrared laser jammers to confuse missiles from locking in on planes.

Original use of the technology: defence

Since their development in the 1960s, an estimated 1 million MANPADS have been produced by more than 20 countries, which have exported them to dozens more. Many of these missiles have been diverted to terrorists and insurgents, who have used them to shoot down military and civilian aircraft, including several large turbojet planes.[65] Efforts to address the terrorist threat from MANPADS date back to the Vietnam war, but until recently, these efforts were largely reactive, modest, and ad hoc. Initially, anti-MANPAD technology consisted of flares intended to produce an IR signature so large that the target signature is overwhelmed, and the seeker locks onto the flare instead of the target. Since MANPADS were becoming more and more sophisticated, other technologies were developed for countering MANPAD launches on planes, especially directed

[65] Christopher Bolkcom and Bartholomew Elias, "Homeland Security: Protecting Airliners From Terrorist Missiles," CRS Report for Congress, RL31741, February 16, 2006; Bureau of Political-Military Affairs, Department of State, "The MANPADS Menace: Combating the Threat to Global Aviation From Man-Portable Air Defense Systems," September 20, 2005 (fact sheet).

infrared countermeasures. Their goal is to overwhelm the signal produced in the enemy missile's seeker by the target, and then to substitute a specially modulated signal transmitted by the laser, so as to divert the missile.

New area of application: civil security

After being in use for over 3 decades on military planes[66] interest in mounting civilian aircraft with similar type of anti-MANPADS technology rose at the turn of the century. Although most MANPADS attacks are aimed at combat aircraft and in combat zones, the number of civilian deaths due to MANPADS attacks has mounted over the years. As the U.S. Congressional Research Service has pointed out, over the past 25 years 35 commercial aircraft have been attacked of which 24 have been shot down, resulting in more than 500 deaths.[67] This led to a number of government initiatives to develop MANPADS countermeasures for civil aircraft. The biggest of these efforts came from the US. After the 9/11 attacks and the attacks on a commercial aircraft in 2002 (Kenya) and 2003 (Baghdad), US Congress and the White House set up a programme to investigate the protection of civil aircraft against MANPADS. It included a $109 million feasibility study by the Department of Homeland Security's to see if anti-MANPADS technology could be made cost-effective for commercial applications. BAE systems and Northrop Grumman were selected for further developing and testing such technologies. Both companies developed a system based on infrared sensors and pulsating infrared flashes (i.e. "directional infrared counter measures") that confuse the incoming missiles. BAE systems developed the *JETEYE system*, which was first flown on a commercial airliner and tested against simulated man-portable air defence systems on the AA Boeing 767 in 2005. Northrop Grumman Group developed the *Guardian*, a commercial edition of its similar system that has been in use by the U.S. military since 2000, and has since equipped 11 FedEx planes with the technology. In 2010, after an investment of $276 million, Congress and the White House quietly stopped funding the MANPAD programme, due to cost issues.

Outside the US, other companies had some success in selling anti-MANPADS technology to the civil market. This was especially so for two Israeli companies, ELTA and ELBIT Systems and had much to do with the government programme for developing MANPADS countermeasures. Since the MANPADS attack on a plane carrying Israeli tourists in Kenya in 2002, the Israeli government increasingly came to see such man portable missiles as a serious threat for its civil airplanes. It decided to award ELTA Systems with a contract for supplying all aircraft (i.e. around 30) of the national Israeli airline EL AL, as well as on board of 2 private airlines flying to high risk destinations with the *Flight Guard system*.[68] The system includes a warning device that scans potential threats in the surrounding terrain of the aircraft. Once a direct threat is detected, a jamming system immediately deploys decoy flares to steer any threatening heat-seeking missiles away from the aircraft and toward the decoy flares. However, the use of flares created safety concerns, leading the Swiss aviation authority to ban EL AL aircraft equipped with the Flight Guard system in the Swiss airspace.[69] In response, the Israeli's has awarded ELBIT Systems a $ 76 million contract to develop a new system using laser jamming technology, based on its *multi-spectral, infrared, countermeasure system* (MUSIC) for military aircraft. The project started in 2008 and resulted in *Civilian-MUSIC* being implemented on all Israeli civilian airplanes as of 2011 on costs of the Israeli government. The system comprises a missile warning sensor, a thermal camera to acquire and track the target, and a fiber laser that generates the jamming beam.[70]

---

66 http://www.globalsecurity.org/military/intro/manpads.htm.

67 http://www.ifri.org/files/CFE/CFEbolkcom.pdf.

68 http://www.upi.com/Business_News/Security-Industry/2009/09/18/ELTA-fits-Flight-Guard-on-Israeli-jets/UPI-59981253288263/#ixzz1ej7Bn3oX.

69 http://www.ynetnews.com/articles/0,7340,L-3221013,00.html; http://en.wikipedia.org/wiki/Flight_Guard.

70 http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=comm&id=news/ISRAEL062609.xml&headline=Israeli%20Airliners%20To%20Get%20Missile%20Defense.

In Europe, SAAB (Sweden) has targeted the civil anti-MANPADS market as well. It developed its *Civil Aircraft Missile Protection System* (CAMPS), equipped with missile approach warning sensors providing 360-degree coverage, with fast-reacting BOA electromechanical dispensers fitted with newly developed pyrophoric decoys. This material is non-explosive, non-pyrotechnic and not hazardous on the ground. The system is currently being used on 3 airplanes, for example on aircraft used for United Nations World Food Programme operations. In general, sales seem to be slowly rising and other European companies, such as the Italian Elletronica (that worked with ELBIT on developing their MUSIC device), are jumping in on Directed Infrared Countermeasures (DIRCM) technologies against MANPADS.

Conclusion

The spin-off of anti-MANPADS technology into the civil security market is a good example of how threat perception can influence demand for spin-off technology. It is no coincidence that anit-MANPADS devices were first sold to Israeli airlines on contract to the Israeli government. The threat of missile launches on airplanes is much bigger in Israel than in, say, the Netherlands. The 2002 attack on an Israeli airplane seems to have been the driving force behind its push for developing and purchasing anti-MANPADS devices for use on Israeli airplanes. Similar programmes were set up in the US, following an increased threat perception in the wake of the September 11 attacks.

Apart from threat perception, the case also illustrates the bigger role of safety concerns in the civil security domain. As was illustrated by the issues evolving around the Flight Guard system, such worries are particularly poignant in civil markets and usually translate into much stricter constraints on the use of military technologies. In this case, the perceived fire hazard from anti-MANPADS technology using flares led to the replacement of such devices by other, “safer” technologies.

A third point is the role of governments in funding R&D and opening up new markets. The Israeli and US government programmes were important factors in developing anti-MANPADS countermeasures that were equipped for civil use. In case of the Israeli government the development programme led to large-scale sales of the newly developed devices. At the same time, the fact that US congress abandoned its MANPADS programme has essentially killed sales to the civil market.

Fourthly, the case points out how costs play a different role in military and civil security sector. Technologies developed for military are often required to be state of the art, with costs considerations of a second order. The civil security industry is much more cost conscious. In this case, the airlines industry very much resisted the obligatory purchase of anti-MANPADS technology. Apart from the purchase costs (somewhere between $500.000 and $1.000.000), airlines have to deal with additional fuel consumption due to added drag and weight. RAND corporation estimated that mounting anti-MANPADS systems on 6.800 US commercial planes (fleet size in 2003) would cost $11 billion in installation and $2.1 billion in annual operating costs.[71] For this reasons, the airline industry was strongly against the obligatory purchase of such systems.

A 2004 report estimated that sales of anti-MANPADS devices for the civil sector would be around $6 billion.[72] 7 years later, that estimate seems to be a way too positive – for example, the CEO of Elletronica estimates the total market size for anti-MANPADS to be around $1 billion.[73] Although

---

71 http://www.rand.org/pubs/occasional_papers/2005/RAND_OP106.pdf.

72 http://www.frost.com/prod/servlet/market-insight-top.pag?docid=18494588&ctxixpLink=FcmCtx13&ctxixpLabel=FcmCtx14.

73 http://www.defensenews.com/story.php?i=6723006.

earlier estimates may have been optimistic, the spin-off market size does seem to be substantial, as is illustrated by companies entering the market with new products, such as the Italian company Elletronica.

4.3.7 *Case 7: Defender M [Protective clothing]*

Technology

Royal TenCate is a Dutch company that manufactures 'advanced materials' (technical textiles) for a variety of products, among them protective fabrics. It offers complete systems based on protective fabrics and advanced armour solutions, including protective clothing. In 2005/2006, Tencate developed their Defender M fabric. This inherently heat- and flame resistant fabric was based on rayon fibers made by Lenzing AG (Austria) for use in military uniforms. The material was developed specifically to protect against burns caused by IED's. In the event of fire or explosion, the fabric is self-extinguishing and will not combust. Its low thermal shrinkage rate helps it to retain its integrity and strength when exposed to flames or high heat.

Original use of the technology: defence

When US troops began operating in combat theatres in Iraq and Afghanistan, limiting the damage done by improvised explosive devices (IEDs) became a prime issue for the US Ministry of Defence. One of the problems was that military uniforms were ill equipped for handling flames and extreme heat resulting from such explosions. The detonation of the IEDs led to more and more serious and life-threatening burn injuries, for which the Ministry of Defense required a quick solution. It set out to award a contract for equipping troops with new uniforms that were more flame resistant. In answer to a solicitation of the Defense Department, TenCate submitted fabrics with several blends of flame resistant rayon, para-aramid and modacrylic fibers in various percentages. TenCate already had experience with producing flame resistant materials in suits for firemen in particular. On the basis of this knowledge, it developed the Defender M at its Southern Mills factory (Union City, Georgia, US), which it had acquired earlier in 2004 and, at the time, was one of the US market leaders in fire, flame and heat-resistant fabrics. In 2005, this led to the Defender M, a para-aramid rich fabric that was both heat and flame resistant and, tests showed, reduced second- and third-degree burns significantly more compared to traditionally used fabrics made of cotton and nylon.[74]

After another solicitation from the US Army, the Defender M fabric was selected as the material of choice for the Fire Resistant Army Combat Uniform (FR ACU) in 2007. Factors influencing the choice for this fabric were: high degree of heat- and flame resistance, durability, comfort, and costs, while at the same time matching other non-FR ACU fabrics in texture and appearance.

TenCate also won a tender for the US Marine Flame Resistant Organizational Gear programme of 2007. Both contracts for the Army and Marine Corps were renewed in 2011. Currently, all US soldiers and marines in combat wear uniforms made with the Defender M technology, totalling 3,6 million uniforms at a cost of $469.3 million.[75] The technology behind TenCate Defender™ M is now also being used in other military branches in and outside the US, such as the US Air Force. TenCate manufactures 11 million yards of fabric exclusively for military applications annually.

Since TenCate started making uniforms with the Defender M fabric for the US military and marine corps, it also attracted other buyers. Other defence actors purchasing similar suits are the Norwegian Navy (+50.000 suits), the Italian Army (+8.000 suits), the Australian Army (+10.000 suits) and the British Army (+300 suits).

---

74 http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWMcd2eLa3PM.

75 http://www.tencate.com/Pages/13371/TenCate/Corporate/en/Home/News/Bloomberg-TenCate---DuPont.

In addition, several extensive wear trials at different (confidential) NATO armies were held. For future sales, Asia is becoming a specific focus point for TenCate. In 2011, it partnered with a local licensed producer in South Korea. Furthermore, it started targeting the Chinese market in particular, e.g. by developing of a new product line based on the Defender M, the TenCate Fire Dragon.[76] [77]

New area of application: civil security

After the development of the Defender M and its sales to the US military, TenCate started to focus on developing fabrics that would address the demands of potential customers for the European and civil security markets. The result was an adapted version of Defender M with anti-static properties, lower weight allowing for patterns in different, dark colours. The latter was especially important for creating a spin-off market. The challenges faced by civil security are comparable with the military threats and requirements. However, for special units (e.g. special squads, riot police) who principally wear solid dark shades for their operations, a new blend of materials had to be developed to allow the product to be dyed in solid dark blue and black. The new blends and colours target the European civil security market and marine corps and police forces in particular.

After adapting the blend and producing prototypes for new suits, TenCate sold substantive amounts of the adapted Defender M for garments to civil security actors, such as riot police and special squads. The spin-off was driven by both end-user marketing and product differentiation, since TenCate purposefully went about adapting its innovative technologies to tap into perceived new market potential. So far, sales have been made to South African fire fighters (+1500 suits) and riot police in at least one western country (+1.500 suits). Again, TenCate is targeting the Asian market and China and South Korea in particular for sales of Defender M to police forces. In addition, TenCate has developed a further spin-off product for the industrial markets that is currently sold in North and South America, Europe, Asia and Australia.

As for market size and potential: in total, sales of the Defender M related products are around 100-150 million euro, accounting for almost 10% of TenCate's total turnover.[78] The global market for advanced protective gear and armour was worth $4 billion in 2010 and the figure is expected to reach $5.2 billion in 2015 at a compound annual growth rate (CAGR) of 6.1%. Thermal protective market was worth $566 million in 2010. This should increase at a CAGR of 5.3% to reach $733 million in 2015. [79] DuPont and Kermel are TenCate's main competitors, but TenCate is a customer of fibres produced by Dupont as well. They all have their own patented fibers and fabrics: DuPont has Kevlar® and Nomex; Kermel has Kermel. Both competitors produce protective fibers and fabrics and are active in the military and security markets.

Conclusion

The case highlights a couple of issues related to international sales of spin-off products. First, one of the issues TenCate has to deal with was trade barriers that limit market possibilities – by, e.g., prohibiting the use of imported materials in civil security garments. For example, potential sales to the civil security market in the US is more limited after the 2009 Kissell amendment, which demands textile products contracted by the U.S. Department of Homeland Security to be manufactured in the US with 100% U.S. inputs.[80] In case of the contract for US military uniforms (won by Defender M), a special waver had to be passed by Congress to allow a foreign company to

---

76 http://www.nonwovens-industry.com/news/2011/09/13/tencate_to_develop_fr_fabrics_for_chinese_market.

77 http://www.tencate.com/TenCate/Corporate/documents/press_releases/2011/110913%20Press%20release-%20TenCate%20concerning%20memorandum%20of%20cooperation%20with%20Chinamex.pdf.

78 *Soldatenpakken van een kunstgraskoning. Volkskrant. 14-10-2011.*

79 http://www.marketresearch.com/BCC-Research-v374/Advanced-Protective-Gear-Armor-6434109/.

80 http://nationaltextile.blogspot.com/2009/01/full-text-and-debate-kissell-amendment.html.

deliver (foreign) technology/materials. Another factor inhibiting spin-off is the frequent demand that production happens in the country of the end user. The fact that TenCate uses many local licensed producers in its consumer countries, such as in South-Korea and the US, partly circumvents this and helps targeting the Asian and US market respectively.

Another lesson is that TenCate was able to sell its technology in another market by focusing on value chain management. It cooperated with other companies, such as Lenzing AG in Austria in developing new blends of fibres for new protective fabrics. The same holds for the spin-off market. By partnering with companies at different stages of the production cycle (e.g. chemical companies producing fibres, factories producing garments), it was able to deliver a more cost-effective and high quality product with potential beyond its initial market. In addition, high investment in R&D (a company wide total of $7.9 million in 2007) allowed it to pro-actively adapt its fabric. This, combined with a focus on end-user marketing, had a positive effect on sales to civil security actors.

4.3.8 Case 8: Taser [Non-lethal weapons]

Technology

Taser is an electroshock weapon that uses electrical current to disrupt voluntary control of muscles. It is classified as non-lethal or less-than-lethal weapons. Its manufacturer, Taser International, calls the effects "neuromuscular incapacitation" and the devices' mechanism "Electro-Muscular Disruption (EMD) technology". Someone struck by a Taser experiences stimulation of his or her sensory nerves and motor nerves, resulting in strong involuntary muscle contractions.[81]

Original use: civil (security)

The original users of the technology were security/law enforcement agencies and they continue to be its largest users. Taser was founded in 1993 (originally as "Air Taser") and, according to CEO Rick Smith, was "your usual start-up story" until it joined with police forces in 1999.[82] Since that time it has been adopted by law enforcement agencies around the world as a non-lethal option that has shown to reduce the level of fatalities and injuries for law enforcement officers and perpetrators alike. TASER claims in its publications that police forces utilizing the Electronic Control Devices have decreased law enforcement personnel injuries by 70% and suspect injuries by up to 79%.

US based company Taser International is by far the market leader and electroshock weapons in general are frequently referred to as the “tasers.” However in recent years other companies have been trying to break into the market including Stinger Systems and Law Enforcement Associates Corporation (LEA). Increased competition in the market for tasers (stunguns), might bring new benefits for law enforcement and civilians.[83]

New area of application: defence

Since the creation of the technology in the early 1990’s the company has continued to develop the technology creating various sizes, strengths, and methods of deployment to branch out into different markets. There are varying versions of this technology that have been formatted for different uses, including projectiles that can be shot out of a customized shotgun.

The spin-off to the defence market was a combination of supply and demand driven. The stabilization missions in Iraq and Afghanistan highlighted the challenges of governing civilian populations with often only lethal force as an option for the military forces. As a result this created a

---

81 http://en.wikipedia.org/wiki/Taser#cite_note-0.

82 http://tech.fortune.cnn.com/2011/09/06/a-new-life-for-taser-this-time-with-less-controversy/.

83 http://robertsiciliano.com/Releases/stungunrelease_July20.pdf.

demand for effective non-lethal mechanisms to protect the soldiers and civilians, similar to the needs that were previously addressed in the law enforcement environment. Simultaneously Taser International was obviously interested in the increased utilization of their product in new markets, so they adjusted the technology for military purposes. One of the main factors that facilitated the spin-off was the fact that the Taser was successful in the civilian/law enforcement sphere in delivering a reduction of injuries and fatalities.

The company offers two main products for military forces, a hand-held TASERÆ Electronic Control Device (that can be affixed to the Picatinny rail system of an M4 or M16 rifle), as well as, Extended Range Electronic Projectiles designed for pump-action shotguns.[84] In addition, there have been Tasers customized for attachment to the front of Humvees to protect the vehicle and its occupants without killing the suspected perpetrator.

Besides law enforcement and military other potential users include civilian self defence, private security, and private military companies. The basic taser (customized for different roles) technology is able to be utilized in hostile conflict zones as a less lethal option in situations that would otherwise lead to the use of lethal force. The current international missions of state-building and stabilization efforts which bring military personnel in frequent contact with civilians make the use of non-lethal weapons an attractive option for military forces.

In the years 2005-2009 Taser saw strong growth in sales, and its revenue in 2009 reached US$104 million. However in 2010 net sales declined to US$87 million. This decrease in sales can be largely attributed to the economic environment as governments at all levels were reducing funding for programs and budgets. To expand the size of the market, Taser has plans to increase market penetration in the United States, as well as the international market. With many law enforcement agencies not yet utilizing Taser's there is definite room for expansion, particularity in the international market.

Taser's international sales have been weak so far. Part of the problem for Taser has been the hesitation of European governments to approve the use of the products by their law enforcement agencies or for civilian usage. One example of Taser attempting to overcome this weakness is by turning its focus to Europe, as attested to by the creation of the subsidiary Taser International Europe SE.

Conclusion

Experience with the spin-off of the electroshock weapons developed by Taser International shows that transfer from the civilian security sector to the military sector proceeded relatively easily within the U.S. assisted by increased focus of the United States military on stabilization operations abroad. The company faced more challenges expanded into new international civil security market in Europe in particular. There is a major difference in the attitudes towards the electroshock weapons from the government, law enforcement and general public in Europe compared to the U.S.

4.3.9 Case 9: LUNA UAV (Platforms)

Technology

LUNA is an UAV system for real-time surveillance, reconnaissance and target location at ranges exceeding 100 km with an endurance exceeding 6 hours. The platform is a lightweight glider of

[84] http://www.taser.com/products/military#operationalUtility.

glass fibre composite material, having a modular payload concept (EO sensors, SAR, photo or video cameras, meteo sensors, CBRN sensors, etc.).

To operate LUNA you need two crews: one launch team and one recovery team. A typical system includes ten air vehicles, two catapult launchers and two vehicle mounted ground control stations. It takes less than 30 minutes to lay out the launch site and launch the UAV. For the recovery a parachute is used. From a virtual cockpit the flight is monitored and controlled. LUNA also transmits images and system data in real-time to the ground station.

Original use of the technology: defence

Since Lawrence and Elmer Sperry carried out the first automatically controlled flight of an aircraft in 1916, military planners have imagined the value of an uninhabited air vehicle that could spy on the enemy or fire at a target without endangering a human pilot. The Cold War stimulated the desire to carry out airborne missions behind enemy lines without possible harm to a pilot. Initial efforts proved unsuccessful. Yet the Cold War and Vietnam War spurred development programmes, which led to the introduction of the first UAVs being used, specifically the Firebee and the Lightning Bug.[85] Until recently UAVs tended to be small and used mainly for reconnaissance. This is being changed as UAVs can now be used for war fighting as well. Until recently, UAVs have tended to be small, so they depend on technology miniaturization even more than their manned siblings. In the 21st century, the technology has reached a point of sophistication that the UAV is now being given an expanded role in war.

While Germany is not one of the main producers or developers of drones, it is gradually positioning itself in the UAV market under the pressure of concrete operational requirements. Experiments in Afghanistan, Iraq and in Kosovo as well as the worldwide fight against terrorism have demonstrated the possibilities and needs for UAV's, especially their capability to provide timely, effective and low-risk reconnaissance and to accurately engage targets in places where the enemy believes itself save and unobserved.[86] One of the UAVs developed for these purposes is the LUNA UAV, which is mainly used for data collection purposes. The UAV is produced by EMT (GE), a certified aviation company, supplier of air vehicles, aviation equipment and unmanned aerial vehicles or drones, comprising the range of micro drones, mini drones and larger tactical drones.[87]

LUNA represents a lightweight glider concept making extensive use of civil COTS components and subsystems to build a system customised to military needs (all-weather, high-performance, modular concept). The articulated and urgent demand from the German Armed forces in operations (Kosovo, Afghanistan) considerably speeded the development. The close cooperation between the developing company and consumer (in this case the military user) helped reducing development time[88]. This resulted in a comparatively cheap UAV system. In addition, LUNA is relatively small, fitting into a jeep-size vehicle, C-130 aircraft and can be deployed by CH-53 helicopters.[89]

In July 2011, EMT stated to have sold more than 500 UAVs including international exports[90]. International costumers of EMT include Norway and the Netherlands[91] and Pakistan[92]. Beside the

---

85 http://www.nasa.gov/centers/dryden/pdf/111761main_UAV_Capabilities_Assessment.pdf.

86 Thiele, Ralph, 'Drones for German Foreign and Security Policy', Institute fur Stategie – Politik- Sicherheits- und Wirtschaftsbertung, Berlin undated. *kms1.isn.ethz.ch/.../Feb2011_**Drones**.pdf*.

87 http://www.emt-penzberg.de/index.php?id=25&L=1.

88 Franz Wasgindt, „LUNA – Eine Erfolgsgeschichte", Strategie&Technik, October 2007.

89 http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=342&zoneid=47.

90 This number includes UAVs other than LUNA (e.g. ALADIN UAV). See EMT press release, "7000. Flug des Aufklärungssystem LUNA", July 2011 http://www.emt-penzberg.de/fileadmin/presse/2011_07_Pressemitteilung_LUNA_1107.pdf.

EMT Ingenieurgesellschaft, many other companies are producing competing products in this emerging market, e. g. AirRobot GmbH (Germany), Finmeccanica (Italy), General Atomics Aeronautical Systems (USA), microdrones GmbH (Germany), Northrop Grumman (USA), and Thales (France). UAVs have been used in military contexts for decades, and more than 90% of expenditures on UAVs have been from the military.[93] In 2011, 1,424 UAVs have been produced in 51 countries by 511 producers/developers[94].

New area of application: civil security

As described by representatives of the development and the funding organisation, the involved parties were aiming to develop a dual-use product from the beginning. Therefore, EMT aimed at producing a marketable and competitive UAV. So far though, LUNA is used by the German Armed forces only. EMT seeks to introduce UAVs including LUNA for civil application[95] and tested them for this purpose including the integration of sense & avoid sensors[96]. This fits a more general pattern. Although an increase in civilian usage of UAVs has been expected for several years, only few European countries have an actual record of civilian testing and/or application of UAVs. For example, Sweden carried out an evaluation of a MALE (Medium Altitude Light Endurance) UAV system helped by military-civilian cooperation in 2002.[97] Other project aimed at developing and/or testing UAVs with dual use purpose or for civil applications include publicly funded projects under the 7th Framework Programme.

EMT sees opportunities for the use of civil security UAV's for the security of power plants, industrial complexes, military bases, protection of waterway's, national border and energy conduit surveillance (such as oil and gas pipelines and electricity networks). In addition the UAVs could be used for monitoring water pollution and the measurement of local radioactivity after reactor accidents.[98]

In recent years, the civil use of UAVs is becoming more and more common, for example:

- The Texas Police department used an UAV during the Super Bowl;[99]
- BAE Systems formed the 'South Coast Partnership' in the UK with local police forces in Kent and Sussex to develop UAVs as part of their policing arsenals. BAE is also promoting the use of UAVs to provide security at the 2012 Olympics in London;
- Switzerland cleared the UAV RUAG ranger for flying in non-segregated airspace, so the UAV can be used for civil task such as border control, fire fighting and traffic monitoring duties by the Swiss policy;[100]
- Other police forces in different countries are using UAVs, for example in South Korea, Brazilian and Mexico.[101]

---

91 Markus Fasse, "Militärische Kleindrohnen erobern den Himmel", Handelsblatt, February 15, 2011, p. 24 http://www.emt-penzberg.de/fileadmin/presse/2011-02-15_Militaerische_Kleindrohnen_erobern_den_Himmel-Handelsblatt_Nr32.pdf.

92 http://ec.europa.eu/enterprise/policies/security/files/uav_study_element_1._en.pdf.

93 Günter Freiwald, "Unbemannte Luftfahrzeuge der Bundeswehr", Seminar at the DHPol, September 7, 2007.

94 Van Blyenburgh, P. (ed.), "UAS – Unmanned Aircraft Systems – The Global Perspective 2011/2012", 9th Ed June 2011 http://www.uvs-info.com/index.php?option=com_docman&task=doc_download&gid=7314&Itemid=20.

95 EMT press release, "Der Nutzen von Drohnen im zivilen Bereich", November 2006 http://www.emt-penzberg.de/fileadmin/presse/november2006_de.pdf.

96 Franz Wasgindt, „LUNA – Eine Erfolgsgeschichte", Strategie&Technik, October 2007.

97 Swedish Evaluation of a MALE UAV-System in Civil and Military Airspace from a Civilian Airport", NATO RTO MP-SCI-162-15.

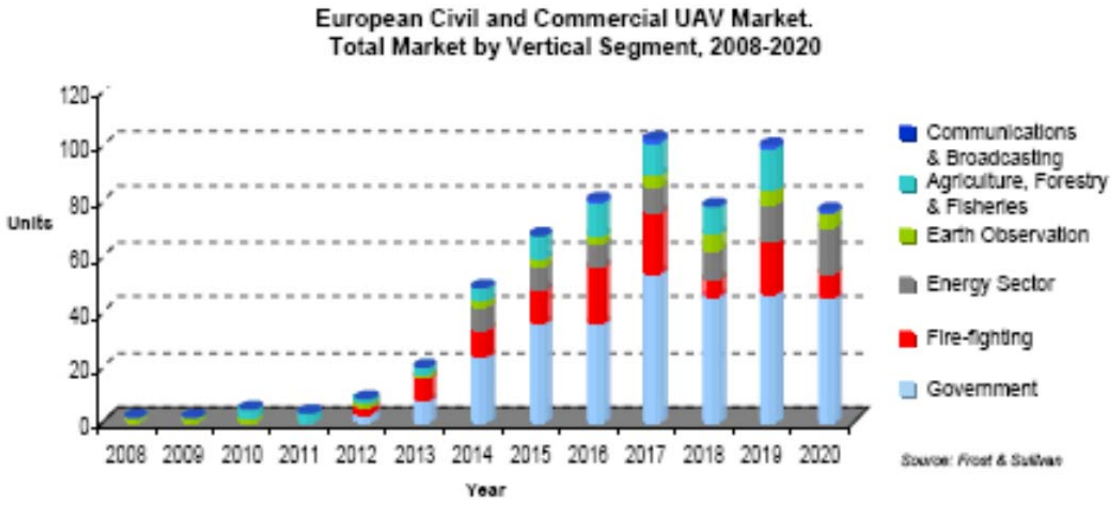
98 http://ec.europa.eu/enterprise/policies/security/files/uav_study_element_1._en.pdf p:34.

99 http://www.auvsi.org/news/fullarticles/.

100 http://ec.europa.eu/enterprise/policies/security/files/uav_study_element_1._en.pdf.

101 http://dmilt.com/docs/UAV.pdf.

This trend is reflected in the graph below, which shows the predicted growth of the civil and commercial European UAV market.[102]



For EMT, the size of the UAV business has doubled in five years to approximately €35 million in 2010[103]. This is in line with market growth estimates. Teal Group's 2010 market study estimates "that UAV spending will more than double over the next decade from current worldwide UAV expenditures of $4.9 billion annually to $11.5 billion, totalling just over $80 billion in the next ten years".[104] A market report of Global Industry Analysts Inc expects a global growth in spending on UAV and Systems of up to $5.34 billion in 2017.[105] Although increasing use of UAV for non-military applications is foreseen, competiveness and market survival of competing companies are strongly dependent on defence spending. Additionally, "efforts of European civil aviation authorities and the FAA [Federal Aviation Authorities] to rationalize civil certification procedures will be a key factor for future growth." [106] The market for civil application is limited to relatively few countries and to a few niches (agriculture, border control, surveillance of infrastructures including pipelines, traffic, and mass events) [107,108]. One of the issues companies like EMT encounter when trying to expand into the civil (security) markets is that, in many countries, UAVs cannot routinely be operated outside segregated airspace.

The military and civil UAV markets are highly interdependent and experience fast technological developments. The European Commission and the European Defence Agency have shown a significant interest in supporting the development of dual-use UAVs.[109]

Conclusion

---

102 Thiele, Ralph, 'Drones for German Foreign and Security Policy', Institute fur Stategie – Politik- Sicherheits- und Wirtschaftsbertung, Berlin undated. *kms1.isn.ethz.ch/.../Feb2011_**Drones**.pdf*.

103 Markus Fasse, "Militärische Kleindrohnen erobern den Himmel", Handelsblatt, February 15, 2011, p. 24 http://www.emt-penzberg.de/fileadmin/presse/2011-02-15_Militaerische_Kleindrohnen_erobern_den_Himmel-Handelsblatt_Nr32.pdf.

104 http://tealgroup.com/index.php?option=com_content&view=article&id=62:uav-study-release&catid=3&Itemid=16.

105 Global Industry Analysts Inc., "Unmanned Aerial Vehicles (UAV) and Systems - A Global Strategic Business Report", October 2011.

106 Aero News Network, "Analyst: Global Spending On UAVs To Reach $5.34 Billion By 2017 - New Report Cites Defense Increases, Growth In Civil Market" November 17, 2011 http://www.aero-news.net/index.cfm?do=main.textpost&id=5657b1ef-03ee-47c2-be8e-4505d4d7e041.

107 http://www.uavdach.org/Anwendungen_e/anwendung.htm.

108 Thomas Petermann and Reinhard Grünwald, „Stand und Perspektiven der militärischen Nutzung unbemannter Systeme", Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, May 2011.

109 http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=5041

The case draws attention to the effect that absence of standards may have on spin-off potential. One of the most often mentioned concerns with regards to the LUNA UAV and other such technologies are safety issues. As we saw in other case descriptions above, safety concerns may limit the attractiveness of a military technology for civil use. The specification criteria that have to be met regarding reliability and safety are often more stringent for civil technologies. This is but one aspect playing a role with the still ongoing change and development of UAV related regulation and legislation. Currently, there are several initiatives to develop and recommend common regulations on different levels, both from the military and civil perspective, as stated in an earlier study.[110] However, there are no pan-European regulations for the operation of military or civil UAVs outside segregated airspace. There are some regulations at national level, but these are not conducive to routine flying activity.[111] In 2007, national UAV air traffic management regulations only existed in France, Sweden, UK, and the USA. A significant change in this market without advances in specification and legislation (including international harmonisation of regulations) is unlikely.

4.3.10 Case 10: Data diode– Fox-IT [Cyber protection]

Technology

This case concerns the Fox-IT DataDiode,[112] a cyber protection technology of the Dutch company Fox-IT.[113] DataDiode consists of a hardware part supported by specially developed software, which makes it possible to transfer information from a lower security information environment to higher security environments. Once the information is in the higher environment it cannot be sent back to a lower security level. For example, once NATO information is received in a Dutch environment, the data from a Dutch environment cannot be sent back to NATO without additional actions.

The advantage of this technology over firewalls and sneakernet (the act of physically couriering data from one security environment to another by using a USB stick or a CD to transfer data) is that the DataDiode technology is not susceptible to human error (such as bugs, misconfiguration, loss of the data carrier) or malicious intent (hacking) since it has made two-way communication physically impossible. Because the hardware component of the DataDiode contains only one optical fibre cable, it cannot physically send data back via this same strand, much like a diode. The advantage being that data can be accessed from a lower security environment, but that the accessing terminal situated in a higher information environment cannot leak information back to the lower security environment.

Should two way communication nevertheless be required, one can place two diodes in sequential order and place a strict content filter between them. Nevertheless, this brings back the risk of data leakage as the content filter may not be airtight.

Original use: defence

The technology was primarily developed for security-conscious government authorities, such as defence organizations, intelligence agencies and the police. The product was first sold to the Dutch Ministry of Defense to communicate in secret with NATO. The main users of the technology are military personnel that needed assistance in their secure communication. Current customers include NATO, the Dutch and US governments. The hardware diode of the Fox DataDiode is listed in the NATO Information Assurance Product Catalogue (NIAPC) and is approved for use up to and

---

110 Frost&Sullivan, "Study Analysing the Current Activities in the Field of UAV - Second Element: Way forward 'What vision can be drawn for Europe in this technology domain and what needs to be done to make it happen', ENTR/2007/065.

111 "Specifications for the Use of Military UAVs as Operational Air Traffic Outside Segregated Airspace", EUROCONTROL-SPEC-0102, July 26, 2007.

112 www.datadiode.eu/technology/certifications.

113 www.fox-it.com.

including NATO Secret (NS). Additionally, the Data Diode meets the 7+ 'Common criteria' standard, which is a European and worldwide acknowledged security certification standard. This standard has levels from 1 to 7, where 7+ is the highest security standard possible.

New area(s) of application: civil security and cross-over

The initial development of the diode has been demand based, whereas the spin-off was supply driven to anticipate on the need for the critical infrastructure protection market. New areas of application are in the field of public critical infrastructure protection, such as (nuclear) power plants and hydro energy suppliers, air traffic control, and public transportation systems. To enter the new market, the diode has been designed to make it possible for operators to receive information for monitoring processes of critical infrastructures in a secure environment. To achieve this, the diode and its software needed only limited customization. New customers were relatively easy to target, since they were already within the network of the company. Other applications can be found in organizations handling tax returns, requiring the secure viewing of financial documents and, much like the security environment of Ministries of Defense and the intelligence community, demanding the protection of (corporate) secrets.

One final application is in the grey area between civilian and military emergency situations. In times of crisis (air plane crashes, natural disasters, toxic spills, riots, etc.) there may be the need for coordination and cooperation between civilian emergency services (low security environment) and military organizations (high security environment).[114,115] The security issue stemming from the necessity of communicating between these divergent security levels may be resolved by data security solutions such as the DataDiode.

The data diode is a relatively new product but already commercially available. At this moment the price for a single diode is around €30,000. Fox-IT expects prices to drop when sales increase. Since R&D investment has already taken place, costs can be spread over a higher volume. At this moment Fox-IT still takes care of their own production and distribution of their product, for both the military and the security market. Their main competitor within Europe is Thales. The (future) sales and total market volumes of all competitors in this product group are still hard to define. However, it is clear to the company that the market outside Europe has shown significant interest in this (and other products) to protect themselves in the cyber domain. It has already teamed up with companies in and outside Europe to provide more comprehensive and custom data protection solutions and (software) add-ons to the DataDiode hardware.[116]

In general, the functional demands placed on military technologies often form an obstacle for spin-off in the field of cyber security. While it would be more cost-efficient for military agencies to buy commercial-off-the-shelf components, which are used in civil security organizations, most of the commercial components do not meet their security demand.[117] This creates challenges for possible future spin-off from civil to military. But it also presents a challenge from military to civil, because civil security actors are generally less interested in the high security aspect, but more in the interested in the features and performance.[118]

Conclusion

---

114 http://www.wil.waw.pl/art_prac/2011/Safe_Exchange_of_Information.pdf.

115 ftp://ftp.rta.nato.int/public/PubFullText/RTO/MP/RTO-MP-IST-086/MP-IST-086-04.doc (The Oasis Approach to Civil/Military Information Sharing for Disaster and Emergency Management).

116 http://www.datadiode.eu/partners.

117 National Research Council, 'Cyber security Today and Tomorrow: Pay Now or Pay Later', Washington D.C.

118 Ibid p. 9.

This case points to three relevant factors affecting spin-off potential. First, spin-off in the cyber security domain is facilitated by the global increase of awareness by governments and large organizations of cyber threats. Second, the interoperability of the product is important. In the case of Fox-IT DataDiode such interoperability seems to be relatively high. It enjoys a wide range of applications, and it can be integrated into custom solutions alongside other software and hardware components to ensure data security. Hence the product can appeal to a wide variety of markets. The final factor is the trade-off between data accessibility versus data security. DataDiode can guarantee that no data is leaked but only in a one-way data transfer setup. A sequential setup enables two-way data transfer but also brings back the risk of data leakage. Customers will have to determine for themselves which aspect they value more.

4.4 Main lessons from the case studies

In this section we address the main lessons that we derived from the case studies in the previous sections; lessons that should be taken into account when seeking to influence and stimulate spin-offs between the military and civil security domains.

Lesson 1. Overlapping 'low end' military and 'high end' security missions open many opportunities for military- security synergies (spin-offs).

The case studies show that the overlapping (or blurring) security and defence missions create opportunities for using products/technologies previously unique to one domain in the other. In many cases new security threats created demand for advanced technological solutions often borrowed from defence. Examples include UAV/UUV, anti-MANPADS devices and sophisticated sensor systems. In other cases, the military focus on stabilisation and reconstruction missions led to the adoption of technologies previously used only in civil security, such as the electroshock weapon.

Lesson 2: The defence and civil security markets differ significantly

Despite the overlap between defence and security missions, the defence and security markets remain significantly different. Some of more general structural differences between the two markets have been already discussed in §2.4. One additional fundamental distinction that comes out of the case studies concerns the driving forces of technology and product development in these markets. The military market is primarily driven by performance maximization: systems and technologies used by military actors must outperform those of adversaries. New defence systems often push the technological frontier forward, with cost concerns playing only a secondary role. The environments within which the military are supposed to operate require more extreme specifications and standards (environmental parameters such as temperature, moisture, vibration, g-force, etc.).

In contrast, the security market is more concerned about cost containment. The civil (security) industry often develops new products using the "must cost" approach (Lorell et al, 2000). Under this approach a manufacturer first conducts market research to determine customer requirements for cost and performance of a new product and then chooses a price target that becomes a binding constraint during product development. Rigorous price targets are also passed down the value chain to the suppliers of various parts and equipment. Product innovation in the civil (security) industry tends to be more incremental rather than revolutionary. Much attention is paid to process and manufacturing innovation and optimization.

Lesson 3: Market differences often pose significant barriers for (potential) spin-offs

Most of the time products developed for one market cannot be used directly in the other. For defence products, the main barriers include very high acquisition and maintenance cost, use of specialized military specifications, and somewhat less regard for comfort, safety and health

standards and regulations. Security (and more generally civil) technologies often have to be ruggedized, made more secure and interoperable with the existing military technologies. Military components are often tested individually, whereas civil components mostly are tested through sampling. The extent of the technical changes required for spin-offs varies on a case-by-case basis.

However, besides technical adjustments that potential spin-offs might require, companies that want to enter a new market face additional 'soft' barriers. One issue that was pointed out in the interviews is that the required marketing capabilities differ significantly for the two markets. In the defence sector, building up long-run relational capital by working with a MoD is essential. In the security sector the demand side is much more fragmented. Responsibilities are split or shared between the Ministry of the Interior, various security agencies, regional and municipal authorities, private sector parties and even citizens. Even large defence companies seem to have been challenged in understanding civil security customers needs and requirements, building networks and marketing strategies. This is also true for the other side – idiosyncrasies of the defence market make it difficult for civil security companies to enter the defence market; this is probably especially true for smaller companies.

Lesson 4: There have been rather few products deliberately designed for both markets from the outset (preconceived spin-offs)

In the examined cases, we rarely encountered technologies that have been developed with both the civil security and military markets in mind. Although it is difficult to be confident without extensive access to internal companies' documents, many of the spin-off cases appear to be opportunistic: companies do not seem to design products for both markets, but do jump on the opportunity when a prospect appears for selling an (adapted version of) the technology. One reason for a limited number of preconceived spin-offs might be directly related to Lesson 2 – large differences between the markets: it seems to be difficult to design for both markets simultaneously.

Lesson 5: Spin-off from military to civil security markets is more prevalent that the other way around

We see much more spin-offs from the military to the civil security markets than the other way round. Given the fact that governments' defence R&D budgets typically are significantly higher than the corresponding public expenditure on civil security R&D (see also Chapter 7) this is not surprising. Defence R&D effort leads to the development of a plethora of innovative defence products that may later trickle down to security markets.

Of course, there is a significant flow of spin-offs (from the civil (commercial) industry in general to defence. This flow is encouraged by several European MoDs that in the last decades have introduced a formal 'off-the-shelf, unless' policy[119] (see e.g. case 5). However, the role of the civil security industry (which is the subject for this study) in this flow is limited.

Most off-the-shelf items represent components rather than integrated systems. At the same time, it is difficult to single out a separate civil security industry at the level of technologies and components. Typically, such technologies and components are supplied by companies for which the civil security market is but one of many customers (and often only a minor one). As a result, we found most of civil security – military spin-off examples at the system or sub-system level rather than at the level of technologies and components (see Charts 3.2 and 3.5) as was to be expected from theoretical considerations (see discussion in Chapter 1).

[119] An 'off-the-shelf, unless' policy holds that the default option is to use technology/products available on the market wherever and whenever possible, with the burden of proof lying with those that want to deviate from this - i.e. start a dedicated technology or product development.

Lesson 6: Government regulation is often one of the main barriers for realizing spin-off potential

Many cases show that regulation can be a very significant barrier for spin-off. We identify the following areas of regulation that played an important role in case studies:

1. **Comfort, health, safety and privacy regulation.** Civil security products typically have to comply with more stringent requirements with respect to comfort, safety, health and privacy compared to military products. Military products often must be extensively modified to conform to such regulation requirements. Many cases show the importance of such regulation. For example, integration of UAVs into civil airspace is closely connected with safety and privacy issues. The use of neutron tubes for baggage screening is restricted by health regulations. Protection of civil aircraft against portable guided missile attack with the flare-dispensing systems raised safety and fire risk issues in the areas close to airports. This makes the application of certain military technology in the civil domain more difficult;
2. **Trade protectionist measures**. Defence and security industries are typically considered as strategic industries by governments. In order to protect their home industries many governments have rules that require the use of domestic production and materials for public procurement in the fields of security and defence. This obviously limits opportunities for most efficient and innovative companies. One example is TenCate case (Case 7) where sales of protective clothing to the U.S. armed forces became possible only after Congress passed a special waver;
3. **Export control regulation**. This regulation is another factor that might have negative consequences for spin-offs. Lengthy and costly procedures associated with export licensing significantly increase time to market and add to product cost. In addition, predictability and visibility of the criteria used by relevant authorities are often lacking. It introduces an additional degree of uncertainty into corporate decision-making and limits potential market size and the cost advantages associated with market expansion. Case 2 (Infrared cameras) is a most visible example where such issues play an important role;
4. **Sensitivity and classification of defence technologies**. Governments adopt stringent rules to protect their technological advantage over potential adversaries, classifying military technologies. As a result these rules might (potentially) prevent transfer of military technologies to civil security, ironically, for 'security' reasons. In Case 6, for example, special kit installed on civil aircraft to provide protection against MANPADS often include sensitive military technologies. Special care should be taken to prevent access to these technologies by unauthorized personnel especially in foreign airports.

Obviously, these regulations address vital societal concerns. In some cases new concerns about security risks (i.e. an increased threat perception) may outweigh safety and privacy issues. This than leads to a revision of related regulations to facilitate the introduction of new technologies, products and procedures. One such example is the increased use of biometrics and surveillance in public places. However, most of the time regulation in the civil sector should be considered as part of the broader environmental differences between the military and civil security markets.

Lesson 7: Many spin-off processes do not follow a direct linear pattern

Spin-off often is not a simple and linear process. We often see (e.g. in case 2) a diffuse 'circular' process of technology transfer between the military and civil markets:

- high-end technology is developed for military-only applications; this leads later to
- limited 'premium' spin-off to niche civil markets; this is followed by
- a market expansion process in which the focus shifts on lowering costs through relaxation of specifications, investment in more efficient production technologies with corresponding large decreases in costs and expansion of the market; this could lead to
- a possible spin-in of cost-effective 'off-the-shelf' products back to the military market.

Case 1 (SODERN's neutron tubes) also shows a convoluted way by which technology can spread. Neutron tubes were initially developed for the French nuclear weapon program based on civil technology. Then, it was adapted for industrial applications and only recently became used in the civil security field. Interestingly, this civil security application then led to new military use (demining). Case 5 – SAAB's 3D Mapping technology case shows a spin-off that took place from the military market to the civil (consumer) market first and only then to the civil security market.

Lesson 8.Sensor systems and C3 seem to be the most fruitful areas for spin-offs

Analysis of the identified spin-off examples shows that two functional areas – sensor systems and command, control and communications (C3) – accounted for by far the largest share of all cases (see chart 3.1). These are the areas where underlying technologies are essentially the same for defence and civil security. They are also quite large in terms of market size. As a result, prominence of these two functional areas is not surprising. See Chapter 5 for a further elaboration of areas with large potential for synergies.

5 Functional areas with large potential for synergies

5.1 Overview

In this Chapter we discuss our approach to identify functional areas with the largest potential for synergies (spin-offs) between the civil security and defence sector and vice versa. There are several ways to identify these areas and different observers might come up with different lists.

Our approach included two main steps. First, and based on the analysis of successful spin-off cases, a review of published studies and theoretical considerations, we have identified the main factors that have contributed to the success of spin-offs in the past. The list of such success factors is quite long and many of them are specific to a particular case. In order to be able to use some of these factors as forward-looking criteria for the identification of functional areas with the largest potential, these success factors should meet the following conditions:

1. They are to be applicable to all (or almost all) functional areas. More specific factors may be very important in individual spin-off cases (or for individual functional areas), but they do not allow a systematic comparison across all functional areas;
2. They can be consistently estimated and show some variation across different functional areas.

The results of our examination suggest that the following four criteria satisfy these conditions and provide the most valuable information:

5. Similar operational needs/requirements in both civil security and defence sectors;
6. Technology level;
7. Market attractiveness;
8. Existing joint R&D.

In the second step the project team conducted a structured expert assessment by applying the above criteria to various functional areas in order to identify those with the largest potential for spin-offs. This assessment was conducted by project experts with the help of other experts in their respective organizations (DECISION, FOI, Fraunhofer, TNO and HCSS). The results of our assessment identify two areas as most promising for spin-offs: cyber protection and sensor systems. In the sequel of this chpater we give a more detailed discussion on these criteria and our findings.

5.2 Criteria

5.2.1 Similar Operational Needs/Requirements

Probably the most important and most obvious criterion for the identification of areas with the largest potential for spin-offs is the existence of operational needs that are common (or similar) to defence as well as to civil security. In the most extreme cases the same system or platform can be used both in defence and civil security without modification or with minor modifications only. Sometimes it becomes just a question of classification or naming. For example, patrol boats designed for border protection roles, such as anti-smuggling, anti-piracy, maritime law enforcement and rescue operations, may serve in a nation's coast guard or police force, but they may also serve in an other country's navy. This can be considered as a civil security-military spin-off, although a rather trivial one. In other cases, spin-offs based on the same operational needs are less trivial,

such as in the case of anti-MANPADS and Defender M fire-resistant uniforms. While being used for defence applications, civil security actors came to see these products as suitable for fulfilling a more or less identical need (i.e. protection of civil aircraft against MANPADS and personal protection of civil first responders).

More often, however, military and civil security needs are similar but not identical. Military requirements typically involve better protection, higher survivability, compatibility and interoperability with existing defence systems and equipment, among others. These differences in requirements often necessitate significant adjustments in order to use a products that was primarily developed for one sector in the other. The extent and costs of required technological (and often manufacturing) adjustments present one of the main barriers for spin-offs. We will discuss this issue in more detail below. Nevertheless, similarities in operational needs (capabilities) provides very obvious opportunities for spin-offs.

5.2.2 Technology Level

As emphasized earlier (see figure 1.1 and related text), significant differences in terms of innovation dynamics exist between the different technology levels[120]. Technology level also plays an important role in the extent and nature of the technological adjustments required for a spin-off to be successful:

1. **Systems and platforms** tend to be designed for specific missions. Unless these missions (or operational needs) are quite similar, spin-offs at the level of systems and platforms are difficult to achieve. For example, civil security and military might use similar helicopters developed from the same basic platform but with different on-board electronic and other equipment (payload). EC-145, a light utility helicopter manufactured by Eurocopter, is widely used for civil security missions by a number of EU member states. It was also selected by the U.S. Army as UH-72 Lakota helicopter for similar missions: medical evacuation, personnel recovery, counter-narcotics operations, etc.[121]. Although it was procured by the U.S. Army as a commercial-off-the-shelf product it still required installation of secure military communication equipment, sensors, engine inlet filters, medical evacuation kits, etc.[122] Spin-offs from military to civil security often require modifications that would make their acquisition and maintenance costs significantly smaller. This can be achieved by relaxing performance characteristics, by using less expensive commercial components and so on. The IRIS case provides an example of how such technological adjustments can be done. By using less sophisticated and cheaper materials the cost of the original military Gatekeeper system was reduced to approximately one tenth of the original. Often manufacturing technology has to be changed and improved in order to make military spin-offs acceptable in terms of price to civil security buyers;
2. At the **equipment and sub-system level** the extent of adjustment during the spin-off process tends to be less substantial because equipment / subsystems are often less specialized than platforms / systems. Nevertheless such an adjustment is still required. The non-lethal weapon case illustrates this point. Spin-off required some adjustments determined by differences in missions but these adjustments were relatively small or trivial;
3. **Basic technologies** can be used across different domains in some cases unchanged. For example, both military and civil security might buy the same microprocessors and basic biometrics technologies are the same in military and civil security. However, not any basic technology is a dual-use technology. Often military and civil security emphasizes different aspects of the same technology. Some technologies are used exclusively by defence (at least

---

120 We distinguish three technology levels: 1) technologies, 2) equipment and sub-systems, and 3) platforms and systems.

121 http://en.wikipedia.org/wiki/UH-72_Lakota.

122 CSIS, Defence Industrial Initiatives Current Issues. No. 7: Case Study – The Drivers of a Successful COTS Acquistion.

for a period of time), for example, stealth technologies or nuclear weapon technologies. Often, the spin-off path for such technologies is not straightforward. The case of neutron tubes illustrates this point well. The corresponding technology was developed for the nuclear weapons programme and only after many years it found potential applications in the civil security and industrial sectors, where it is used for completely different purposes. Nevertheless, our conclusion is that the extent of technological adjustment required for successful spin-off at the lower level of the technological pyramid is typically less significant than at the higher levels. For example, in the Defender M case basically the same suits is used for protection of civil security actors. That some adaptation was required had more to do with “cosmetic” reasons (police forces normally wear blue/black suits instead of camouflaged military versions) then functionality.

The lesser extent of adjustments necessary for spin-offs at the lower levels of the technological pyramid suggests that spin-offs should be easier to implement when dealing with generic technologies rather than with integrated platforms and systems. At the same time it should noted that we do not see many civil security-military spin-offs at the level of technologies/ components (as our list of the cases demonstrates). As it was mentioned, it is difficult to delineate a separate civil security industry at this technological level (with some exceptions). It is typically either civil (not civil security per se) or defence companies that operates at this level. Therefore, at the level of generic technologies and components one often sees general civil-military spin-offs rather than civil security-military spin-offs.

5.2.3 Market Attractiveness

The size of the potential market, its expected growth rate and demand uncertainty are important factors in judging the potential for spin-offs. A large and growing market, with limited volatility in demand, provides more incentives for manufacturers to enter the market and justifies larger investment in technical adjustments necessary to create a spin-off than a small and declining market.

It should be noted that the market demand in defence and to a large extent in civil security is created by the governments. Perceived risks of various security threats is reflected in the level and the allocation of funding for the military and security forces. Perception of security threats can change dramatically as a result of accidents. The 9/11 attack in the United States led to the creation of a new Department of Homeland Security and a dramatic increase in security funding. Terrorist attacks in Europe had similar but smaller effects. Governments often react to new security threats by adopting more stringent safety and security regulations. This might have a strong impact on the market size. Since 9/11 the airport security procedures became much more thorough creating, for example, more demand for better security screening equipment.

However, importance of the same security threat can be perceived quite differently in various countries. For example, anti-MANPADS systems were first sold to Israeli airlines on contract to the Israeli government, where the (perceived) threat of portable missile attacks against civil airplanes is much higher than in the EU.

Demand uncertainty is also likely to be quite important for companies when they decide to invest in spin-offs. If new security expenditure or security regulation adopted in the wake of a terrorist accident are perceived as fleeting then private long-term investments in adjusting military products for civil security needs are less likely to be made than in the case when companies see a long-term commitment from the governments. Long-term capability plans and technology roadmaps for the

civil security domain (see Chapter 8) could provide more certainty in terms of future demand for the industry.

5.2.4 *Joint R&D*

Another criterion that might be important in judging the future potential for spin-offs is the existence and extent of joint civil security – military R&D effort. Such efforts:

1. Indicate early interest of both sides in the potential product/functionality;
2. Help to address specific requirements of civil security and military early on;
3. Develop a culture of working together.

It can be expected that existing joint R&D projects will result in a number of commercialized spin-offs later on. As a result it can be used as a forward-looking criterion to determine the functional areas with a large potential for spin-offs. Space, CBRNE protection, cyber security and C3 are the areas where many cooperative projects with defence and civil security participants are taking place and where the flow of civil security-military spin-offs could intensify.

5.2.5 *Other Possible Criteria*

There are, of course, other factors that might play an important role in the spin-off process, such as:

- Similar demand side of the market;
- Previous experience with civil-military spin-offs within the organization;
- Need for cross-border EU-external cooperation (e.g. in disaster response);
- Timing aspects (TRL, procurement schemes);
- Role of classified information and restrictions on dual-use technology exports.
- Role of safety and privacy regulation, etc.

For several reasons, it is difficult to use these as criteria for assessing functional areas. Often their role in the spin-off process can be judged only on a case-by-case basis and cannot be reliably estimated for a functional area as a whole. Some of them might have a very similar impact across all functional areas. Sometimes their importance is less clear cut than for the criteria that were described earlier.

Governmental safety and privacy policies provide one example. They play a very important role in the spin-off process. Some of our cases illustrate that currently such policies might pose barriers to spin-offs (the neutron tubes and non-lethal weapons cases). They might also become significant demand drivers for spin-offs from civil security to military domain, if more stringent safety norms are to applied to defence equipment and systems. However, given large volume of health and privacy regulation the impact of such norms is impossible to judge across functional areas in general without detailed, case-specific investigation.

Another example concerns intellectual property rights. The rules on IPR for publicly funded R&D projects can obviously have a large impact on potential spin-offs. However, it is not obvious that these rules have a consistently different impact for different functional areas. Therefore, IPR rules are not helpful as a criterion for selecting promising functional areas.

5.3 Assessment

To identify the potential for spin-offs across the functional areas we use two main approaches. The first one is based on the results of a simple analysis for the identified spin-off cases (Chapter 3). The second one makes use of a structured expert assessment and based on the criteria listed above in this Chapter.

It should be clear from the outset that our selection of spin-off cases cannot claim statistical representativeness that is necessary to reach general conclusions. It rather provides an indication of the functional areas with the highest spin-off *potential*. This analysis is also purely historical, i.e. it reflects insights derived from spin-offs that have already happened (with some exceptions), leaving the forward looking nature of this assessment debatable. These caveats notwithstanding, it is interesting to note that both a broad scan of spin-offs and in-depth case studies consistently demonstrates that two areas had the largest number of spin-offs (charts 3.1 and 3.3):

- **Sensor systems;** and
- **C3.**

This broadly matches the functional areas (sectors) with the largest market size (for high level security) in the Ecorys study on the Competitiveness of the EU security industry (Ecorys, 2009).

Next we conducted an expert assessment of the functional areas with the largest potential for spin-offs. A questionnaire that listed the functional areas (Chapter 2) and the criteria identified in this Chapter was sent to all project partners. This questionnaire had to be filled in consultation with relevant experts from their organizations (Decision, FOI, Fraunhofer, HCSS, TNO).

Received questionnaires were aggregated and a simple statistical analysis was performed. We initially assumed that all criteria have equal weight but it was shown that plausible variations in weights assigned to different criteria do not change the results much. It was found that two functional areas received scores substantially higher than the others:

- **Sensor systems, in particular biometrics;** and
- **Cyber security.**

They scored much higher than other areas in terms of similarity of operational needs in civil security and defence and typically performed no worse than other areas against the remaining criteria.

This result is not surprising. The market in these two areas is large and has been growing quite rapidly. Capability required by defence and civil security in these areas are broadly similar. In both areas lower technology levels –technology, equipment, components and sub-systems – are significant.

It should be noted that there is a close overlap between the expert assessment and the results of the case analysis. Sensor systems are present in both; C3, one of the top areas in the case study analysis, and cyber security, which came as one of the two most functional areas in the expert assessment, have a lot in common especially at the lower technology levels.

6 General Framework for Industry Assessment of Civil-military Synergies (Economic Models)

6.1 Introduction

The aim of this Chapter is to outline and assess the role and influence of civil-military (technology) synergies on industry (firm) behaviour and development approaches. We identify some of the main factors and characteristics that might influence the realisation of such synergies; specifically in terms of the extent of transfers of technology between the defence and civil-security domains. In particular, we focus primarily on technology spin-offs, which we treat in a broad way that encompasses both the spin-off of a particular technology from one sector to another and at a more general level of company diversification strategies into different market sectors.

6.2 Overview: general scope, concepts and definitions

In attempting to set out a general framework to describe the main factors and characteristics that may – from a business perspective – influence the realisation of civil-military synergies, the multi-dimensional nature of the issues to be addressed becomes quickly evident. These dimensions include *inter alia* the range of categories ('functional areas', see §3.2) of relevant technologies; the levels of technology development and integration at which a spin-off may occur (see §2.3); the distinction between synergies originating from the specific attributes of technologies and synergies originating from their means of production; the range of client-categories making up the market for defence and security products; and the types and sector-origin of companies supplying products to defence and security markets, etcetera. Accordingly, in the following sub-sections we attempt to outline some of these dimensions in more detail.

6.2.1 'Top-down' versus 'bottom-up' approaches to the identification of potential civil-military technology synergies

In general terms, the assessment of the potential for civil-military (technology) synergies can be approached from two directions. First, a 'top-down' (operational) approach that is based on an assessment of the threats and risks in the defence and civil-security domains and the consequential definition of defence and security missions and priorities, including the allocation of responsibilities among the various defence and security actors to fulfil different missions. In turn, such an assessment provides for the identification of the corresponding capability requirements and means required by the military and civil-security sectors to address the missions allocated to each of them. Following a 'top-down' approach, potential civil-military technology synergies arise through commonalities in operational capability requirements and technology needs. Software Defined Radio (SDR) is one area that provides an example of common capability requirements for military and civil security forces and where the European Commission and the European Defence Agency have initiated efforts – particularly in relation to the definition of common capability and interoperability requirements – to foster potential synergies in the development of SDR technologies. More broadly, looking beyond specific technologies, synergies may be realised in terms of common systems architectures or modular systems architectures adapted to both military and civilian requirements. Synergies may also be realised through common procurement processes for the civil and military sectors although, in practice, this seems to be a rare occurrence. Following a 'top-down' approach, the scope of potential synergies evolves in response to changes in the

threat and risk perceptions in both the military and civil-security areas that have the effect of altering the perimeters of common capability requirements and technology needs. In this respect we can speak about mission or capability-driven changes that alter the potential for technology synergies.

Secondly, a 'bottom-up' (industrial) approach based on an assessment of the technological and other capabilities available within firms or, more broadly, at the level of industrial sectors. Following a 'bottom-up' approach, the potential for civil-military synergies is driven by the opportunities for industry to apply its technological capabilities (e.g. 'know-how', components and products, production tools) across both the military and civil-security domains. At the same time, as will be discussed further on, it is not sufficient that an opportunity exists for a firm/industry to apply its capability technology.[123] In general terms, the scope of potential civil-military synergies evolves alongside technological developments – including both technological advances per se and in their means of production– that augment the range, functionality or affordability of available technologies that may be applied in the areas of defence and civil-security[124]. More specifically, the scope for potential for civil-military technology synergies in terms of spin-offs between sectors will evolve as technological developments primarily aimed to one sector of application lead to the creation of opportunities for their application in other sector(s). In this respect we can speak about technology-driven changes that alter the potential for technology synergies.

Evidently, the actual potential for civil-military synergies will be determined by the intersection between 'top-down' (or demand-side) requirements and 'bottom-up' (or supply-side) capabilities to deliver technologies that accord with these requirements. In this respect, the 'top down' approach towards defining mission and capability requirements is far more established within the defence sector than in the security sector; as is the understanding of the capabilities and capacities of the defence industry. Efforts towards 'top down' identification of requirements in the security area are, by and large, far more recent, less well established and less systematic. This is also the case for the identification of potential (operational and technological) synergies between the defence and civil security sectors; for example, the French 'Livre Blanc sur la défense et la sécurité nationale' (2008) or the UK's 'Strategic Defence and Security Review' (2011) and recent 'National Security Through Technology: Technology, Equipment and Support for UK Defence and Security' (2012).

6.2.2 Firm-level versus technology-level civil-military synergies

In this section, and in common with the rest of this report, we will focus mainly on a 'bottom-up' (technology-driven) or *industry-orientated* approach to the assessment of civil military synergies. In this respect, two inter-related levels of analysis of technology-related synergies between the civil and military sectors can be distinguished:

- **Level of firms:** i.e. where synergies may be realised through the diversification of a firm's activities across different sectors. In this regard, a central question is why firms choose to diversify their activities; for example, why have some defence firms more actively sought to

[123] The realisation of synergies requires, also, that the opportunity is recognised and that firms develop the necessary complementary capabilities to turn a (potential) opportunity into a product that will be attractive to the target mechanism. Or, alternatively, that some other mechanism exists through which a potentially interesting technology can be brought to the market.

[124] The driving force behind advances in technology may come primarily from the military or civil security area, or from outside either of these. In this regard, it is worth recalling the point made earlier that (generic) technologies are essentially 'neutral', in the sense that they are not inherently military or civilian. However, the application of a technology within a specific area can remove – or at least reduce – this neutrality when it imposes characteristic on the technology that can restrict the possibility of its application in other areas. Restrictions on the diffusion of technologies may occur due to the fact that a technology is initially developed or applied in a particular sector; i.e. the sector from which a technology 'originates' may influence the possibilities for diffusion. Furthermore, the level of integration of a technology (e.g. from component-level through to platforms and systems) may impact on diffusion possibilities due to the fact that higher levels of integration typically imply greater degrees of customisation to meet specific user requirements.

enter the civil-security market than others (and why have some companies have been more successful than others in doing so)? In turn, what are the main factors influencing firms' diversification strategies? In particular in the context of this part of the study, to what extent may these strategies be influenced by potential technology-related synergies arising through diversification?

- **Level of technologies:** i.e. where synergies may be realised through the diffusion of a specific technology from one sector to another sector. In this regard, a central question is why certain technologies originating from one sector are more rapidly adopted in another sector? In turn, what are the main factors influencing the speed of diffusion of a technology and how do these factors relate to the characteristics of the technology? In particular in the context of this part of the study, to what extent do potential synergies influence decisions over whether and how technology development (programmes) and technology diffusion are pursued?

6.2.3 Technology development versus production-based civil-military synergies

In setting out the general conceptual framework underlying this study, a distinction was made between different levels of technology – or levels of technological integration. This distinguished between (generic) technologies and subsequent higher levels of integration, culminating in platforms and integrated systems. This also points to a distinction between synergies that take place due to the 'intrinsic' attributes of a technology[125] (i.e. its contribution to meeting specific capability requirements) and synergies that occur at the level of products with, where necessary, with appropriate adaptation to meet particular market requirements. Based on this distinction Table 6-1 provides a general classification of technology-related 'synergies' resulting from technology development and the associated production of ('high tech') goods. This classification can be used for synergies between the defence and general civilian sectors in general as well as for synergies between the defence and civil security sectors in particular (since we consider the civil security sector a subset/part of the civilian industry)

The first level of Table 6-1 identifies synergies arising out of knowledge and technology development processes, which correspond essentially to outcomes of research and development (R&D) efforts. Three sub-categories of interaction between military and civil (security) R&D can typically be identified[126]:

- **'Spin-off' technology:** i.e. technologies developed through military R&D efforts that also find applications in the civilian sector;
- **'Spin-in' technology:** i.e. technologies developed through civilian R&D efforts that also find applications in the military sector;
- **'Bridging' technology:** i.e. technologies developed with the purpose to fulfil both military and civilian applications or, more loosely, technologies for which their application to military and civilian sectors go hand-in-hand even if this was not an express purpose at the outset. The source of R&D may come from either the military or civilian sector or both sectors together.

Essentially, the defining criterion for each of the above categories relates to the initial or predominant purpose of the technology development effort. Hence a 'spin-off' (or 'spin-in') infers that the origin of a technology is attributed to a particular sector. By contrast, in this classification, a

---

[125] In other words, what is important for realising a synergy are the intrinsic attributes if the technology to contribute to meeting a specific capability requirement and not the product (component, equipment, system, etc.) in which the technology is embedded.

[126] For the purposes of classification, the term 'spin-off' is used to refer to technologies developed for military purposes that have subsequent civil, including civil security, applications. The term 'spin-in' refers to the mirror image process, whereby technologies developed for civilian purposes have subsequent civilian applications. Elsewhere throughout this Report, the term 'spin-off' is used irrespective of the direction of diffusion of technology between sectors.

'bridging technology' is one that it is developed with the purpose of addressing both military and civilian applications/requirements or, for which, its application to both sectors emerges before it takes on a specific 'military' or 'civilian' connection. In this respect, a fundamental difference between a 'spin-off' (or 'spin-in') and a 'bridging' technology, is that the former presupposes that the development of the technology – at least the initial stages – has to some extent already been undertaken. Consequently, some level of R&D investment has already been foregone before the 'spin-off' (or 'spin-in') takes place. By contrast, there is no such presupposition attached to the development of a 'bridging' technology.

The second level of Table 6-1 relates to the location of production of 'goods'[127] and provides a similar three-way sub-categorisation of military and civilian interaction, based on the sectoral location of production:

- **'Buy-in' production:** i.e. goods produced for civilian purposes that are used in military applications. The most obvious example being the utilisation of 'commercial off the shelf' (COTS) components and sub-systems within military systems;
- **'Sell-on' production:** i.e. goods produced for military purposes that are used in civilian applications;
- **'Joint' production:** i.e. goods produced expressly for both military and civilian applications. The location of production may be in either the military (defence) or civilian sector, or both sectors together.

As with the synergies at the level of knowledge and technology development processes, a distinction between 'buy-in' (or 'sell-on') production and 'joint' production is that the former presupposes that production destined for one market is already taking place before the 'diversification' to the second market occurs. In general, for both 'generic' technologies and products there exist a distinction between technology synergies arising from the diffusion of existing technologies – with appropriate adaptation – from one sector to another and the development/production of new technology destined for multiple sectors.

Table 6-1 Civil-Military interaction in technology development and production

Activity / Technology ('integration') Level	Defence	Interaction ("synergy")			Civilian (Civil security)
Knowledge and technology development ("technology transfer")	Military R&D	→	'Spin-off' technology	→	Civilian R&D
		←	'Spin-in' technology	←	
		←→	'Bridging' technology	←→	
Production (e.g. components, equipment, sub-systems, systems and platforms)	Military (Defence industry) sector	←	'Buy-in' (e.g. COTS)	←	Civilian (high-tech industry) sector
		→	'Sell-on'	→	
		←→	Joint production	←→	

Source: adapted from Brzoska (2006).

The classification presented above draws a distinction between synergies arising from technology development and those arising from production activities, based on their sectors of origin and

[127] We use the term 'goods' in a generic sense that can refer to either or both the embedding of technology within physical products of the codification of knowledge/technology, for example for IT software and systems.

destination. It does not, however, examine the actual mechanisms through which this interaction is achieved. Nor does it consider what other complementary conditions may be required for synergies to actual be achieved. However, it should be stressed that for technologies or products to move from one market to another is not simply a question of whether the opportunity for a 'spin-off' – or the other categories of synergy described in classification – exists but, also, on a variety of other conditions and investments that may be necessary for companies to make in order for them to bring a technology/product to a new market.

Following from the above, if we consider the case of a defence company that is seeking to 'spin-off' a technology / product to the civil (security) market, then this may require not only adaptation of its defence technology / product to meet civil (security) market requirements but may also entail significant investments to actually bring a product to the market. In this respect, a criticism of a too simple view of 'spin-offs' is that it ignores also the competences required by defence companies to bring a product to the civil (security) market and may underestimate what is required to develop such competences. In terms of the interaction that firms may be required to undertake in order to access different market segments it is perhaps relevant to make a distinction between technologies/products that serve as 'intermediate inputs' as opposed to those that represent 'final products'. In general terms, we can distinguish:

- Generic technologies and components are 'intermediate inputs' in the sense that there is no final (end) market demand per se (i.e. they are 'supplied' to other parts of the production / value chain);
- Equipment, sub-systems, integrated systems and platforms are 'final products' in the sense that they correspond to final (end) market demand (i.e. they are 'supplied' to end-users)[128].

The point here is that firms that are suppliers of 'intermediate inputs' need not directly interact with the final customer market while a higher degree of interaction is necessary for 'final products'. Thus, the position that a firm occupies within the supply chain of a technology/product is likely to influence the competences and investments necessary for it to supply different market segments. As noted in general conceptual framework underlying this study, in general the higher the level of integration of a technology with a particular product (e.g. as the technology 'moves up' towards systems and platforms) the more difficult it may be to realise potential synergies as the design and specification of the product emerges from a closer relationship between the supply-side (firms) and the demand-side (users/procurement authorities). In this respect, it is perhaps also worth noting that while there is a tendency to consider 'spin-offs' – or the other categories of synergy described in classification, above – in terms of organic diversification of companies from one sector to another based on final products, the actual processes may occur through more complex relationships within supply chains. Moreover, firms may occupy different positions within the supply chains for different market sectors such that, for example, they may supply final products to one market segment and intermediate inputs to another market segment.

6.2.4 Business modes for developing civil-military synergies

There are a number of ways (modes) through which companies may seek to diversify their activities. IAI (2010) notes three following routes through which, for example, defence companies may seek to enter into the security market. These may be applied more generally to cover firms diversifying from and to different market segments. The three modes mentioned by IAI (2010) are as follows:

[128] This does not preclude that equipment and sub-systems may also be considered as 'intermediate inputs' when they are integrated within larger systems/platforms.

- **Organic diversification:** a company enters a new market/sector by drawing on its internal resources and capabilities to exploit already existing technologies. Such organic diversification is likely to rely heavily on the company's capacity to find its own channels to market and to develop the necessary marketing capabilities through trial and error learning, gaining a gradual understanding of the 'new' market;
- **Diversification through acquisition:** a company enters a 'new' market through acquiring other companies that already have relevant technologies/products and an established market position among customers in the 'new' market;
- **Collaboration (partnering/ teaming/ joint ventures):** a company leverage of its own technologies or capabilities through partnering or teaming-up with other companies in order to create a complementary package of market knowledge and/or capabilities to enter a 'new' market.

Large defence companies both in the U.S. and in the EU have been using all three modes to enter the security market in the 'post-9/11 era', when many defence companies foresaw a strong increase in demand for 'high-tech' security products and the possibility to leverage their knowledge of defence technologies. Some examples of recent acquisitions and joint ventures in this area are listed in the table 5.2. Since major prime defence contractors are significantly bigger than even largest security companies (i.e. companies which rely on the security market for most of their sales) there has not been much the activity in the opposite direction, i.e. security companies buying defence firms.

Table 6.2 Recent examples of acquisitions and joint ventures by defence companies in the security sector (in the EU and the US)

Companies	Date	Firms acquired	Domains
EU			
EADS	2005	Nokia's Professional Mobile Radio activities	Secure telecommunication
	2006	Sofrelog (FR)	Vessel Traffic Service systems and Coastal Surveillance Systems
	2008	PlantCML (US)	Emergency response solutions and services
	2010	Atlas Elektronic (DE)	EADS and Atlas Elektronic merged their subsidiaries Sofrelog and Atlas Maritime Security, respectively, to form Sofrelog Atlas Maritime Security in order to consolidate their activities in the maritime safety and security market
Thales	2007	Rail signaling and security systems business of Alcatel-Lucent	
	2008	n-Cipher	Encryption (Internet and communications system security market)
Safran	2008	Sdu-Identification (NL)	Secure identification documents, including electronic and biometric passports, ID cards and driver licenses
	2009	Motorola's biometric business (US)	Printraktrade trademark, automated fingerprint identification systems
	2009	81% of GE Homeland Protection (US)	Systems to detect dangerous or illicit materials (X-ray tomography detection systems) with much of the technology designed for use in airport screening
Finmeccanica	2007	VEGA Consulting Services Ltd (UK)	Project management and advanced solutions for simulation and training
	2008	DRS Technologies (US)	Vessels Traffic Management Systems, port security, law enforcement, border control; subcontractor to Boeing on

			SBInet
BAE Systems	2008	DETICA (UK)	Technologies for analytical decision support, real-time situational awareness and control, secure computing and communications (anti-terrorism and anti-fraud applications)
	2000-2009	More than ten acquisitions in IT, defence electronics and land armament sectors in the USA	
USA			
Boeing	2008	Digital Receiver Technology	Digital signal processing products
	2008	Ravenwing	Cybersecurity solutions
	2008	Kestrel Enterprises	Data management, development and systems integration, programme management, training
	2009	eXMeritus	Hardware and security software
	2010	Argon	C4ISR and combat systems
	2010	Narus	Cybersecurity solutions
Raytheon	2009	BBN Technologies	IT, sensor systems, and cybersecurity
Lockheed Martin	2006	SAVI Technology	RFID equipment and solutions
	2007	Management Systems Designers	IT and scientific solutions
	2008	Eagle Group International	Logistics, IT, training and healthcare services
	2009	Gyrocam Systems	Gyro-stabilised optical surveillance systems
	2009	Universal Systems &Technology	Interactive training and simulation, technical solutions
SAIC	2009	Spectrum San Diego	Ultra-lo-dose X-ray scanning systems
	2010	CloudShield Technologies	Cybersecuirty and management solutions
General Dynamics	2009	Axsys Technologies	High performance electro-optical and infrared (EO/IR) sensors and systems and multi-axis stabilized cameras
L-3 Communications	2002	Perkin Elmer	X-ray scanning business
	2006	CyTerra Corporation	Advanced through-wall radar and explosive detection sensors for checkpoints
	2006	SafeView	Non-invasive scanning systems
	2006	TRL Electronics (UK)	Secure radio and satellite communications for defence and homeland security applications (electronic counter measures and cryptographic areas)
Northrop Grumman	2007	Essex Corporation	Signal processing servicesand products, advanced optoelectronic imaging
	2007	Xinetics	Active optics such as deformable and hybrid mirrors, advanced systems for real-time control of active optics
	2008	3001 International	Geospatial data production and analysis

Source: adapted from Masson and Marta (2011)

The aforementioned three approaches all imply that the company diversifies its activities through some form of direct involvement within the 'new' market. However, technology synergies may also be realised without direct involvement, for example:

- **Third-party mechanisms (e.g. technology licensing):** through which the company does not directly diversify its activities but grants rights to (or sells-off) its technology to a third party through, for example licensing its technology or setting up a joint-venture. This approach recognises that the company may possess valuable technologies but rather than capitalising on the value of these assets through its own diversification/collaboration activities, may prefer to 'spin-off' the technology to a third-party. Typically, such an option is pursued when the potential application of the technology is outside the core business of the company, and a number of major defence-contractors (and civilian companies) are pursuing strategies in this direction. Technology licensing is the main route to commercialize newly developed technologies including security related technologies by a number of defence R&D&T organizations including Defence Science & Technology Laboratory (via Ploughshare Innovations)[129] in the UK, TNO[130] in the Netherlands, Rafael Development Corporation[131] in Israel. In the United States Office of Technology Transition within the Department of Defence[132] is tasked with promoting the commercialisation of defence technologies including their application for homeland security[133].

6.3 Factors and conditions influencing industry (company) approaches to civil (security) - military technology synergies and market diversification

The preceding Section has sought to set out some of the relevant dimensions of potential (technology-related) synergies between the civil and military sectors. In this Section, we move towards a discussion of the factors that – from a more business-orientated perspective – may influence industry (firm) behaviour and development approaches. In line with the general scope of this study, we will focus primarily on synergies between civil security and defence rather than between these sectors and the wider and more general civilian environment.

Notwithstanding the focus on synergies between civil security and defence, it is relevant to note the reversal of the 'traditional model' in which technology synergies were associated with the flow of technology from the defence to the civilian sector. The rapid increase in the pace of technology development in the civilian sector implies that it is now much more likely that synergies will arise from the flow of technology from the civilian sector to the defence (and security) sector. Although it remains the case that major defence contractors may still be linked into early stage (low TRL) technology development programmes, it is generally the case that their role is not one of 'inventing' new technologies. On the contrary, their role tends be that of adapting or engineering a new technology or innovation to meet military requirements rather than generating the new technology or innovative 'idea' in the first place. This shift in emphasis towards bringing new technology to the defence market rather than directly creating new technology for the market has, also, important implications for the relationships that major defence contractors need maintain with sub-suppliers and partners in the supply chain. Essentially, these sub-supplier and partner relationships play an increasingly important role as a source of new technologies and innovations for the defence sector.

It is also relevant to recognise that there is a strong motivation for demand-side actors to promote civil-military technology synergies. Not least, public authorities – specifically ministries of defence – are keen to promote civil-military technology synergies as a means of reducing procurement costs.

---

129 www.dstl.gov.uk/pages/144

130 http://www.tno.nl/groep.cfm?context=kennis&content=IP&laag1=IP

131 http://www.rdc.co.il/ and Harvard Business School Case: Rafael Development Corporation – Converting Military Technology to Civilian Technology in Israel, 9-602-011, February 2002

132 http://www.acq.osd.mil/ott/index.html

133 Report to the Congress on the activities of the DoD Office of Technology Transition, 2006, pp. 18-26, http://www.acq.osd.mil/ott/techtransit/reports/OTT_August2006_Congressional_Report_Complete.pdf

This is reflected in on-going efforts towards the increased use of COTS and MOTS components and sub-systems in military equipment and systems. Such efforts are primarily concerned with cost savings from the integration of essentially purely civilian technologies in defence – and, to a lesser extent, civil security – equipment and systems rather than from synergies between civil-security and military sectors. More broadly, there is an acceptance that costs for public funding of R&D (and subsequent procurement) may also be reduced if synergies can be achieved through better coordination of military and civilian – including civil-security – research and technology development activities. Further, notwithstanding the financial implications of possible synergies, there exists also the possibility that a more systematic approach to civil-military technology development may enhance capabilities overall. This may be the case, for example, where interoperability between civil and military equipment and systems is required.

6.3.1 General requirements for firms seeking to develop technology synergies and diversification across markets

A basic pre-condition for a firm seeking to pursue a technology-based spin-off is that it must possess a technology that correspond to the common needs of both sectors. Accordingly, for example, there is no basis for defence companies to enter the security sector unless they possess technologies that correspond to the needs of the security sector. For this reason, the fact that a company possesses strong technologies for one sector of application is not a sufficient basis for entering into another market. What is required is a technology that is valuable for both sectors. Of course, changes in capability requirements and technology needs (e.g. as a result of changes in threat assessment and the corresponding definition of security/defence missions and priorities) may alter whether a particular technology is considered valuable by a sector, thus creating potential new opportunities for companies to enter the market.

The fact that a company possess a technology for which there is a need in a sector is not in itself sufficient for successful market entry. This requires, also, that the company's technology has some competitive/commercial advantage over its competitors. There are evidently a range of characteristics that come into play when determining the competitive advantage that a particular product/technology may possess vis-à-vis its rivals. Obvious characteristics include the range of relevant performance attributes and relative price but may include, also, factors such as accompanying support services; flexibility and interoperability etc.[134]

Following from the above, there are a number of other aspects that may be required for a technology to be successfully transferred from one sector to another. These include, for example, the extent to which it is compatible with the general environment ('world') of the potential adopter. For example, IAI (2010) notes the importance of characteristics such as compatibility with existing skills (e.g. whether users in the new market have the required skill set to use a technology effectively or if substantial training is required), existing practices (e.g. operational doctrines and modes of operation), existing organisational processes (e.g. potential disruption to business processes that may be caused through adoption of the technology), and values and norms of potential adopters (e.g. safety, privacy, data protection and other similar issues).

In short, there is a wide variety of general characteristics of a technology that can be expected to influence the feasibility and likely success of efforts towards diversification (spin-off) between markets. In common with most other sectors, these characteristics can be expected to affect the

[134] Another area where it is sometimes assumed that defence companies may have a competitive advantage derives from their experience at a higher architectural level (e.g. systems integration/engineering, networked technology, etc.). IAI (2010) notes, however, that such competences may be found in other sectors such as telecommunications.

role and influence of civil-military (technology) synergies on industry (firm) behaviour and development approaches.

6.3.2 *Specific factors and conditions influencing technology-based synergies between security and defence*

Turning specifically to technology-related synergies between the defence and security sectors, the case studies tend to indicate that synergies (technology 'spin-offs') have occurred more through serendipity than as a result of systematic business approaches aimed at generating technology synergies between the security and defence sectors. Rather than being the outcome of active business strategies, the case studies suggest that where synergies between military and security technologies have been observed they are more likely to be the result of a fortuitous 'accident', 'unforeseen' demand arising in the spin-off market or in response to contractions in demand in the main – typically defence – markets.

Given the relatively short timeframe over which the civil security sector has taken on its present form, it is necessary to be somewhat cautious in drawing conclusions on the potential for future synergies on the basis of observed past behaviour. Further weakening of the separation between military and civil-security missions and capability requirements should *a priori* provide an increased rationale and greater opportunities for technology-related synergies between the two sectors. However, despite such 'demand-side' developments it is far from clear that military and civil-security technology suppliers currently consider that there are many areas where there are viable and compelling business cases for actively pursuing technology-related synergies between the two sectors. Even among the larger defence and aerospace contractors that have sought to build a bridge between their defence and security related activities it appears that it has often been difficult to leverage technology developed for one market (typically, but not exclusively, defence) for applications in the other sector.

The fact that serendipity rather than active business strategies appears to lie behind many observed technology synergies between security and military applications suggests that, in reality, firms find it difficult to integrate the potential for such synergies into business decision making processes. This raises questions as to whether there are specific characteristics (or barriers) of the security and defence sectors that inhibit firms from pursuing market diversification between the two sectors and hence limit the potential for technology-related synergies to be created. In this respect, industry representatives point to the fact that the significant differences in market conditions and requirements for defence and security can contribute to inhibiting the transfer of technology between the two sectors. Among the factors that differentiate the two sectors, the following have been highlighted as having an influence on industry approaches to technology synergies and market diversification:

- Governments (Ministries of defence) are the single national buyer in the defence sector whereas the security sector is characterised by multiple owners and buyers of security equipment and systems; these include inter alia national and local public authorities, infrastructure operators and other private enterprises. Moreover, defence procurement processes are mature and based on established centralised approaches whilst the general immaturity of the security sector means that there may be little in the way of established approaches to procurement;
- The defence market is characterised by specific organisational arrangements that reflect the monopsony position of governments as customers, the corresponding dependence of prime defence contractors on their government customers, and the fact that this situation together with the limited overall size of demand may inhibit the development of a competitive market. Not least among these arrangements, it is more typical for government customers to fund

investments of R&D and thereafter guarantee a minimum level of demand for defence products and systems. By contrast, although public funding for civil-security R&D has increased, investments in technology development for the security sector tend to be financed primarily by supplier firms themselves based on their own assessment of the expected market;

- Defence technology (equipment and systems) needs are identified using centralised 'top down' approaches based a longer-term strategic vision of mission responsibilities and capability requirements and priorities. By contrast, technology needs in the security sector tend to arise in more amorphous ways reflecting the requirements of individual buyers/owners. In general, planning horizons in the security sector tend to be shorter in the security sector than in the defence sector and are more affected by changes in the general economic environment and specific events (e.g. security events and new modes of security threats). Furthermore, the security market is often strongly conditioned by regulatory environment, the development of which is also often uncertain;
- The multitude of both public and private demand-side security segments and the process of evolving requirements make it more difficult to develop a clear picture of current and expected future technology needs than in defence sector. In general this makes it difficult for firms to evaluate market opportunities in the security sector. In addition, some segments of the security sector are characterised by weak demand side capacity to identify their capability requirements and/or to understand the capabilities that a particular technology can deliver or to recognise the benefits of innovative approaches. By contrast, the defence sector is characterised by a high level and more centralised knowledge and understanding of technologies among customers and/or scientific and technology support organisations;
- The difference in demand side structures implies that quite different approaches are necessary when it comes to the marketing and commercialisation of products destined to the security market compared to the defence market. For defence companies, for example, the relational capital built-up through years of working for customers in the defence sector counts for little when dealing with most civil-security customers. Thus, in addition to technological capabilities, companies seeking to diversify into new markets need also to invest in the non-technological capabilities necessary to develop a position on the market;
- Defence procurement tends to emphasis the periodic development and replacement of complete systems whereas procurement processes in security tend to be more incremental and based on updating or extending existing capabilities through the acquisition of additional equipment rather than the complete overhaul of existing systems. Correspondingly, development cycles in the defence sector are long, with the introduction of major new systems measured in terms of decades and characterised by a partnership between the client and supplier from the outset of the technology development processes. By contrast, the security sector is characterised by short development cycles with the competitive advantage conferred by technology developments and innovations measured in months rather than years. Equally, customers tend to have little direct engagement in technology development processes;
- The focus on a whole systems approach in the defence sector tends to strengthen the position of major prime defence contractor as the primary interface with government customers, with their main role and capabilities coming in terms of systems engineering and integration. Notwithstanding the relations that these prime contractors may maintain with a network of sub-suppliers, this structure raises issues in relation to the access of SMEs to defence markets. In contrast, SME's tend to be more prevalent in the supply of final products to the security sector, reflecting the greater fragmentation and more open characteristics of demand;
- Although the more holistic approach to defining equipment and system needs in the defence sector may facilitate longer run technology development/engineering programmes it may, as a consequence, make it more difficult to incorporate new technologies and innovations In general, there is a perception that – having defined capability/technology requirements – defence sector customers may be 'locked-in' to given technologies which makes them relatively inflexible when

it comes to the introduction of new technologies and innovations. Thus, there is little incentive for firms to try to independently develop technologies for defence applications but which are outside the expressed technological capability requirements of defence customers;

- Operational performance requirements – rather than technology requirements per se – and market attitudes towards the deployment of technology are often quite different between the security and defence sectors. For example, defence equipment requirements emphasise that technology must work at the moment it is needed, even if it is to be stored and only used once ('one shot' reliability). Security equipment is more likely to be deployed on a regular or on-going basis (continuous reliability). Even for essentially similar technologies, the nature of essential capability to be delivered may differ between the sectors; for example, for sensors deployed for defence purposes the priority may be to identify if a threat exists whereas for security purposes it may be more important to identify the kind of threat that may be present. In general, it is often the case that the underlying technology required for defence and security applications is the same or closely similar but the global operational performance requirements are different, necessitating quite different engineering approaches;
- Both the security and defence sectors are characterised by high levels of secrecy which, in itself may limit market transparency regarding technological capabilities. In particular strict secrecy conditions regarding defence related technologies are seen as a constraint on their diffusion towards civilian – including civil security – applications. This situation may be further reinforced by explicit controls, such as export bans on defence and other sensitive technologies. Thus, although a technology developed for one sector (typically defence) may have applications in another area this may be prohibited. Alternatively, such considerations may limit the extent to which suppliers are able to demonstrate the effectiveness and performance of their technology. It may be the case that this leads to situations in which suppliers have to make an explicit choice between whether they seek to develop a technology for one sector; for example firms may decide not to develop a technology for military purposes if this would subject the technology to defence sector secrecy requirements that would prevent its supply to the civil (security) market;
- The security sector is often considered to be more price sensitive than the defence sector. In this respect, the defence market is sometimes said to be characterised by a 'design-to-performance' approach whereas 'design-to-cost' is more applicable to the security sector. In general, customer choices over different technologies/products will involve a trade-off between various dimensions, not least in terms of performance vis-à-vis purchases and operating costs. However, customer choices over these dimensions are conditioned by the range of available products on the market. For example if a defence company develops a low-cost variant of a technology/product designed for the more price sensitive security sector, it may find that its existing defence customers choose to adopt the cheaper variant also. In this respect, there may be risks attached to developing technologies for different sectors in terms of the possible 'knock-on' effects on existing markets;
- Market perceptions and general public attitudes to companies and their products can be influenced by the sectoral origin of firms. For example, some potential civilian sector customer may attach a negative perception to products obviously stemming originally from defence sector applications. Alternatively, for civilian sector companies there may be reluctance to diversify into the defence market if there is a potential that this may in some way damage the image of the company and its products in the eyes of its main non-defence sector clients.

Overall, the significant differences in the structures of supply and demand in the security and defence sectors are seen to make it difficult for firms to develop common business approaches to the two sectors and for companies with business models developed to operate in one market environment to enter into the other market. For companies that are familiar with the more coherent and strategic approach in the defence sector, significant adjustments to their business strategies

may be required to accommodate the more fragmented and amorphous conditions in the security sector. For companies operating in the security domain – or, for SMEs technology suppliers in general – the general structure and procurement arrangements and cycles are seen as factors inhibiting access to the defence sector. Further, the controls and limitations that governments may place on the exploitation of technologies for non-defence purposes is also seen as an important consideration for technologies with potential applications in both areas, particularly where the size of the defence market is relatively small compared to civil (including civil security) markets.

6.4 Conclusions

Declining military budgets and, particularly in the current economic environment, structural weaknesses in security budgets can be expected to push both procurers and suppliers to seek to exploit potential synergies in security and defence technologies. Nonetheless, so long as significant demand and supply side differences exist between the two sectors, it is likely that industry will encounter difficulties in simultaneously addressing both markets, both in terms of technology development activities and in the realisation of production efficiency (e.g. economies of scale) that may bring down costs.

One of the most significant factors to inhibit industry stakeholders from developing coherent business approaches to spin-offs between the security and military sectors is the absence of a 'top-down' approach for identifying capability requirements and technology needs in the security sector. Thus, it may not be so much a case of barriers that limit market diversification but, rather, the difficulties and uncertainty that firms encounter when trying to evaluate the expected returns from developing technologies for application in the civil security area. The development of a longer term vision and 'roadmap' for security technology requirements that could be set alongside those developed for the defence sector would enable potential areas for technology synergies to be identified, together with a better appreciation of overall market potential. Such an approach could, and should, go hand-in-hand with and contribute towards efforts to reduce fragmentation in the security sector at national levels and across the EU as a whole. Overall, this should reduce the level of uncertainty attached to industry efforts to develop or adapt technologies for the respective markets, in particular the security market. A more coherent and consolidated approach across the defence and security sectors, combined with greater consolidation within the security sector, could also contribute to increasing the overall potential market open to new technologies and technological innovations that should also stimulate industry efforts towards developing synergies between security and defence.

The general consensus among industrial stakeholders consulted for the study is that greater clarity of security market technology requirement and expected demand levels, together with clarity and openness of the processes and procedures for accessing markets ('route to market'), would encourage industry to more systematically integrated the potential for technological spin-offs into business strategies. Under such conditions, other possible policy initiatives that may be considered to support the promotion of synergies between security and defence (e.g. standards, R&D funding programmes, etc.) would be more likely to have a positive effect.

7 Description of Policy Options

7.1 Introduction

The Commission has requested to study four main policy options for enhancing civil-military synergies and provide their impact assessment:

5. More systematic coordination of research activities between FP7 and EDA through the European Framework Cooperation;
6. Improved upstream coordination at the level of capability development through high-level stakeholder group;
7. Downstream coordination via development and use of 'hybrid' standards;
8. Use of Article 185 TFEU[135] to support joint research effort.

Options 1 and 4 address the issue of more efficient and coordinated R&D effort, especially at the EU level. Option 2 can be applied at the technical level but also at the organisational and architectural level. Finally, Option 3 can address a number of issues and might be helpful in creating conditions for possible future synergies.

After discussing these options in little more detail in the next four sections, the final section of this Chapter identifies some possible alternative policy options that might serve to address some of the issues derived from the case studies (see §4.4). These other policy options are not described in any detail, nor are they assessed for their possible impact in the next Chapter, but only serve as initial food for thought.

7.2 More and more systematic coordination under EFC

The Commission could continue to coordinate research activities between FP7 and the EDA through the European Framework Cooperation for Security and Defence (EFC), but in a more systematic way than is the case today. Currently, the Commission and EDA try to avoid duplication and create complementarity of their respective projects in a rather ad-hoc way and for only a few areas/projects. So far, the Agency and the European Commission have cooperated in the areas of Software Defined Radio and the insertion of Unmanned Aerial Systems into regulated airspace[136] but as of today (April 2012) the EFC itself only covers CBRN. In a quantitative sense, enhancement of EFC implies an increase in the number of areas/projects that might cover many of the functional areas in this report. In a qualitative sense, it would mean moving from a case-by-case and ad-hoc cooperation to an approach that allows for a more systematic coordination and synchronisation. Among other things, this could mean that results from projects on the Commission's side directly feed into projects on the side of the EDA, and vice versa, with final outcomes that are more than the sum of parts.

---

[135] Article 185 TFEU states: "In implementing the multiannual framework programme, the Union may make provision, in agreement with the Member States concerned, for participation in research and development programmes undertaken by several Member States, including participation in the structures created for the execution of those programmes."

[136] http://www.eda.europa.eu/Aboutus/Howwedo/Civmil/EFC

7.3 Promote Hybrid standards

For the civil security market, the role of standards may be summarized as follows: “standards are often a prerequisite for a good performing market. Standards developed by European (CEN, CENELEC, and ETSI) and international bodies are required in a market where network effects are relevant and suppliers and solutions easily cross national borders. Their importance is recurrently stated in the ESRIF (2009, p.198) and EOS (2009) documents. ESRIF suggests a kind of European Security Label that certifies that equipment fulfils standard; EOS suggests European Reference Solutions to guide industry. The development of certification schemes for ICT security products, processes and services is also recommended by IDC (2009:10). The lack of common standards and certification bodies for security in Europe, a task being today a responsibility of member states, could be a relevant weakness that would need some kind of public action. Ecorys (2009:24) attributes this shortcoming to the authorities’ desire to retain control over technology in order to protect domestic industry or avoid dependence on external technology supply, but it may well be due to a weak perception of advantages of a European approach”(Sempere, 2011).

Under this policy option, the Commission could take the lead in formulating and establishing European standards in some or possibly many the functional areas, and in promoting the use of those standards in both the civil security and military domain.

Synergies between civil security and military domain could be fostered by standardisation at the technical, architectural and organisational level. Below, we use the word ‘standards’ and ‘standardisation’ for all these levels; however, it should be noted that at the architectural and organisational level, it is often more appropriate to refer to ‘good practices’ rather than (strict and univocally prescribed) ‘standards’. Keeping in mind the differences between the civil security and the defence market (see §2.4 and Chapter 5), our general assessment of the possibilities of standardisation at the various levels are as follows.

There is a growing spin-in of civil technologies and components, and therefore of civil standards, into the military market. However, the role of the civil security market as a possible intermediate agent in the transfer of technology between the civil market in general and the military market is very limited. **Standardisation at the technical level (technical interoperability and syntax standards)** is therefore not so much a question of conformity between the civil security and military sector, but rather a process of taking advantage of the on-going market drive across the civil sector towards ‘open’ standards and achieving technical interoperability between security and military systems, equipment and applications

Standardisation at the organisational level[137] or organisational interoperability standards[138] should aim at achieving greater interoperability between civil security and defence organizations via harmonisation of corresponding protocols and procedures. It is facilitated by similarities of missions and tasks - and therefore operational needs - between the civil security and military domains. Indeed, increasing overlap between ‘high end’ civil security and ‘low end’ military tasks is evident. There are three tendencies that could accelerate the process of organisational interoperability standardisation.

Firstly, the clear distinction between civil (societal) security and international (including military) security is fading. The conceptual blurring between the two also leads the notion of ‘comprehensive

[137] This level is also known as the functional or procedural level

[138] European Commission, Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards, M/487 EN, Brussels, February, 2011.

security' as an integrated policy domain. In recent years, various European countries have produced a national security strategy, covering a wide range of security risks and threats. Secondly, the actual deployment of military forces in civil security missions and of civil security agencies in stabilisation missions. Military and civil first responders are working together in several on-going missions, thereby providing a practical stimulus for more interoperable systems and procedures. Thirdly, the severe pressure on defence budgets across Europe leads to emphasis on 'value for defence money' in quite a few of the EU member states. The need for 'affordable solutions' could bring the two markets closer together – and at the same time enhance the significance of non-security civil COTS products/components/subsystems. These trends all point towards an increased potential for harmonization of organisational requirements across the civil security and military domain.

A modular approach to missions, tasks and capabilities lies at the heart of organisational interoperability standards. 'Modularity' is nothing new, but the concept has gained importance in recent years because it helps organizations develop adaptability in turbulent environments. Certainly in the military domain, it has become fashionable to think in 'modules' or 'building blocks' that are part of a 'toolbox' which, as a whole, offers the flexibility to face a range of challenges and tasks through proper combination of such modules into new, tailor-made configurations or 'task forces'.

Standardization or, more appropriately, harmonization at the architectural level is called for to achieve uniformity in approach. An example is the Service Oriented Architecture (SOA) approach, stemming from the field of software engineering but becoming increasingly popular as a paradigm for developing complex systems. In the military realm, the so-called network centric or network enabled approach is an umbrella concept for various ways to link distributed functionality across the battlefield. However, the network enabled concept is not confined to military missions, and could well span both the military and the civil security domain. It might be envisaged that standards are being developed that define a minimum common denominator for networked enabled operations in the comprehensive security domain. Harmonization at the architectural level would drive standardisation at the lower (technical and functional/procedural) levels since it can only be fully achieved with technical and organisational interoperability standards in place. For instance, the network enabled approach could push standardisation from technical protocols for communication and information exchange at the basic ICT-infrastructure level (technical interoperability and syntax standards), to high-level Concepts of Operations that define e.g. common data models and specify common service characteristics.

Multi-level security (protection of classified information) is an important notion to address, and a potential barrier for the process/institutional arrangements for standards development in the defence and civil security domains. In particular, ESO's (i.e. CEN, CENELEC, ETSI) use an open process for standards development, which may be inappropriate given the sensitivity of security standards (e.g. classified information). This raises the issue whether and how modalities could be modified to address standards development in the defence and civil security arena.

7.4 Establish a high-level stakeholder group

A high level stakeholders group would incorporate the main actors from the supply, demand and end-user side from both the civil and the military sectors. The challenge, of course, is to set clear and meaningful objectives, terms of reference and a working agenda for such a group. For example, the aim of a stakeholders group might be to identify those areas where common requirements for civil security and military end-users could be set, and common research,

development and procurement initiated. This identification process might lead to synchronized projects under EFC, or to establishing areas where standardisation might be beneficial.

Two avenues could be taken to create buy-in and coverage. In a 'broad' approach, stakeholder invitations should extend to domains that are non-security, but do have distinct security issues, such as transport and communications. In a 'deep' approach, representatives of the EU Member States and of the defence and security industry should be directly represented to balance priorities set at the European level. Of course, the 'broad' and 'deep' approach could be combined, although probably requiring a more elaborate organisational set-up.

In discussions with stakeholders as part of this project, the option for a stakeholder group was not seen as something that can be easily implemented in the short term. At the heart of this diffidence lies a chicken-and-egg kind of problem: on the one hand a high level stakeholder group might be instrumental in trying to overcome the fragmentation of the security domain; on the other hand, that same fragmentation is one of the main obstacles to create a fair representation and a shared agenda for a high level group.

Even so, establishing a high level stakeholder group could accompany several of the other options described here. Depending on the final outcome regarding the most promising areas for cooperation and synergy promotion, the framework for this group should be defined, establishing the intended size of the group, selection criteria, the process for group formation and the working procedures.

7.5 Use Article 185 TFEU

Article 185 of the Treaty on the Functioning of the European Union (TFEU) states that: "In implementing the multi-annual framework programme, the Union may make provision, in agreement with the Member States concerned, for participation in research and development programmes undertaken by several Member States, including participation in the structures created for the execution of those programmes." [139]

Implementing Article 185 TFEU in the Seventh Framework Programme implies that participating EU Member States integrate their research efforts by defining and committing themselves to a joint research programme, in which the EU promotes the voluntary integration of scientific, managerial and financial aspects. The EU provides financial support to the joint implementation of (parts of) the national research programmes involved, based on a joint programme and a dedicated implementation structure.

7.6 Other policy options

The proposed policy options only partially address the structural barriers for increased synergies (see discussion in Chapters 3 and 5, and Conclusion 9 in Chapter 8). One of the main barriers for creating synergies between the defence and the civil security domain is the lack of a longer term perspective and technology roadmaps in the security domain. Development of such a perspective is primarily a national level responsibility. Indeed, a number of national initiatives are under way to

[139] "Consolidated Version of the Treaty on the Functioning of the European Union," Official Journal of the European Union, 30.02.2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF. More information on the use of Article 185 can be found on: http://cordis.europa.eu/fp7/art185/home_en.html.

address that barrier. Some Member States have started a process of developing some sort of "capability based planning" approach, similar to the one cultivated in the military domain over many years. In addition, these Member States have started comparing military and security capacity development plans and are looking for shared road maps to delineate dual technology needs. These sort of efforts can be seen, amongst others, in France, the United Kingdom and the Netherlands[140]. Such national initiatives on military-civil security synergies indicate that, despite obvious difficulties, conditions exist for implementing a meaningful policy reform in the field. A first alternative policy option would be for the Commission to coordinate with the Member States that have already launched concrete initiatives, for example, by facilitating exchange of best practices and lessons learned. The Commission may also take the lead in initiatives that would stimulate a 'Capability Based Planning' approach for civil security mission areas where the EU has political and operational responsibilities, such as FRONTEX.

A second alternative policy option could be to streamline regulation. Regulation plays an important role, for example, in promoting standards. Such standards should be established in the interplay between regulators and market parties.

Another important area is health and safety regulation, which lies at the national and the EU level. For some spin-off examples existing regulation clearly forms a significant barrier. Revisiting existing regulation might be beneficial, but it should be done only a case-by-case basis since such regulation has a very important role in the society.

A final suggestion was for the European Commission to consider the establishment of a European industrial database of available dual use technologies in Member States and R&D projects on technologies and products being developed for civil security and military application in the Member states and at the European level. This would better inform industry concerning available technology in other Members States, to include in further product development across the two markets. Such a database could lower the walls between the markets, and reduce duplication of efforts.

[140] For example, National Security through Technology: Technology, Equipment, and Support for UK Defence and Security (Cm 8278), February 2012.

8 Impact Assessment

8.1 The current defence and security market

Currently, publicly available data collected on the security and defence industries are relatively sparse, with the two main sources being a report by Ecorys in 2009 on the competitiveness of the security industry and a study published in 2011 by the European Organisation for Security. Each of these studies offer figures for 2009 as well as forecasts to 2020.

The general size of the security market depends on its definition, with estimates ranging from €49.2 bn to €103 bn. The larger figure takes into account "physical security protection", which are not counted in some definitions, including the use of CCTV; access control equipment; intrusion and detection systems; and protective clothing.

Defence total expenditure in the EU reported by the EDA (for 26 participating Member States, excluding Denmark) amounted to €194 billion in 2009. This includes approximately €41 billion spent on equipment procurement and R&D.[141] Three countries with the largest defence budgets – France, the UK and Germany – together account for approximately two thirds of all defence investment (equipment procurement and R&D) in the EU. Their dominance is even more pronounced in terms of defence R&D expenditure – their share of the total €8.4 billion was 90%.

However, globally the United States is by far the largest defence market that represents approximately 75% of all NATO's countries defence equipment expenditure.

Table 8-1 Military Procurement Expenditures, 2010[142]

Country	US$ million (current dollars)
United States	188,599
China*	20,022
France	15,605
United Kingdom	15,110
Russia	12,609
Germany	8,572

The trade body for European defence firms – the AeroSpace and Defence Industries Association of Europe (ASD) – provides another look at the size of the European defence market and defence industry.[143] Total turnover of European Aerospace and defence industries in 2010 was €162.9 billion. These companies directly employed 704 thousand workers.

.

In terms of international competition, the most important competitor for the EU is the United States. American companies do not hold the largest share of the world market, but they offer, like

---

141 http://www.eda.europa.eu/Libraries/Documents/National_Data_Breakdown_Publication_pMS_1.sflb.ashx.

142 * –- for 2008. Sources: For NATO countries- NATA Statistics, http://www.nato.int/nato_static/assets/pdf/pdf_2011_03/20110309_PR_CP_2011_027.pdf. Russia – official budget calculated at 2010 US$/RUR exchange rate; China - http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf.

143 ASD, Fact and Figure 2010.

European companies, innovative, high-end security equipment. While Israel and Japan have strong positions in this area, they generally cover niches such as IT and communication security. China and Russia are important in the security field, but they produce mainly low-end security equipment.

8.2 Military and civil security R&D

In Europe, in 2010, around €8.56 billion was spent on military R&D with France, UK and Germany to take account for about 90% of this amount[144].

EU-level civil security research started in 2004 when the European Commission launched its three-year Preparatory Action for Security Research (PASR) with a budget of €45 million for 2004-2006. PASR's purpose was to test the idea of using EU funding for security R&D projects. This paved the way for today's fully fledged European civil security research theme in the EU's 7th Framework Programme for research (FP7) for 2007-2013, with a budget of € 1.4 billion[145].

The European Commission has linked security with economic development since the mid-1990s, and since this time, they have espoused economic efficiency as an approach to increasing security. This link can partly be explained because defence falls largely under the Member State level, but also because of the increasing recognition that technologies originally intended for the defence sector have also been used in other sectors, most notably in non-military security. As early as 2004, members of the European Security Research Programme recognised these principles of civil-military synergies of civil and military technologies, stating: "In Europe, there has been for long a strong separation between research for civil purposes and that for defence objectives. Today, many technologies are 'dual-use': civil developments adding to defence capabilities, developments originally made for defence purposes leading to major innovations and benefits in the day to day life of the citizen. [...] A coherent security research programme at the level of the European Union can add significant value to the optimal use of a highly competent industry" (European Commission, 2004b, p. 4).

One of the primary instruments for the European Commission used to exploit these dualities has been to fund various research programmes , with the Framework Programmes at the centre of the strategy (Lavallée, 2011). The original scope of this FP7 mission was civilian, but by the mid-point of the programme, dualities between civil and military technologies were already being recognised, with two primary examples being:

- Software Defined Radio with applications for both military and civil first responders (police, fire service, and so forth);
- A project on using Unmanned Aerial Vehicles in civil airspace (Bailes and Depauw, 2011).

Some of these successful projects led European Defence Ministers to ask the European Defence Agency to establish the European Framework for Cooperation (EFC) to encourage more of these types of projects that could leverage military and civil technologies. While the goal of the EFC has been to encourage research & development, specifically bringing actors together, cooperation between the European Defence Agency and the European Commission remains separated, with each side maintaining independent frameworks, budgets, and rules. Some aspects are, however, shared, such as objectives and information. Other areas have already been considered for further development, such as: situational awareness (sensor technologies, command and control of

144 Source. EDA Defense data portal.
145 Source. ESRIF final report 2009.

networked assets), maritime surveillance, and protection against chemical, biological, radiological and nuclear threats (James, 2011; Drent & Zandee, 2011).

At a national level, eight countries currently have a national security research programme: Austria, Finland, France, Germany, the Netherlands, Romania, Sweden and the UK. An evaluation of the European Security Research Programme indicates that the European annual funding allocation is larger than all of the national security research programmes combined, which vary significantly. However, some countries allocated a significant budget, such as Germany (€129 million for 2007-2009) and Finland (€160 million for 2007-2013)[146].

8.3 Civil-military synergies

The case studies indicate that, to date, the majority of spin-offs observed is from the military market to the civil security market. The typical economic and social impacts (either positive or negative) that are observed of such spin-off processes in the different cases and from the interview programme are:

- An increase of R&D expenditure by industry: the typical military products need to be adapted to the needs of the civil security market;
- An increase of marketing and promotion costs for industry to enter the new market, which is fragmented (civil security) or difficult to enter (defence);
- A decrease of overall production costs for industry by relaxing specifications and investing in efficient production technologies;
- An increase of sales for industry by:
  - Increased sales in the country of origin;
  - Increased intra-European sales;
  - Increased exports outside Europe by:
    - Improving the competitive position of European industry.
- An increase of procurement costs for security equipment,
- and sometimes a decrease of security personnel costs (due to automation) for civil security end users, as a result of:
  - more available systems and subsystems for civil security end users.
- A decrease of procurement costs for civil security end users as a result of:
  - An increase of joint procurement with military end users.
- A decrease of procurement costs for military end users as a result of:
  - An increase of the availability of commercial, off-the-shelf products;
  - An increase of joint procurement with civil security end users.
- Improved cooperation between civil security end users and military end users as a result of:
  - Improved interoperability of systems;
  - Joint system requirement development;
  - More opportunities for joint training.
- An increase in employment in the civil security and defence industry, as a result of:
  - Additional sales.
- A decrease in employment at end users in civil security and defence, as a result of:
  - Increased uptake of systems by end users that enable automation of their tasks.
- An increase of the overall level of security for society in Europe, as a result of:
  - An increase of available systems and subsystems for civil security end users.

[146] Source: Centre for Strategy and Evaluation Services, Ex-post evaluation of PASR and interim evaluation of FP7 security research, 2011.

The case studies also indicate that the potential for civil-military synergies has yet to be fully realised, as a number of barriers still hamper other spin-offs or the impact of existing spin-offs. The barriers identified from the case studies are:

- **Export control regulation.** This hampers spin-offs from realising further intra-European sales and exports outside Europe. This was seen in two case studies on sensor systems and protective clothing;
- **Health, safety and privacy regulation.** This prevents the application of certain military technology in the civil domain. This was, for example, seen in the case of neutron tubes;
- **Lack of knowledge of civil markets.** Some organisations may have technology that would be of interest in a civil (or military) case, but may not have the knowledge or network to understand how to approach these new clients. Adapting a product to client demands is not the issue, but rather understanding fully how to reach those clients. The prime case example here is the 3D mapping;
- **Fragmentation of the civil security market.** The demand side is often comprised of regional or local governments with different requirements;
- **Idiosyncratic defence market.** Long term relationship between MoD and industry, with industry often sharing the risks of system development;
- **Secrecy rules for Defence companies.** As indicated in Chapter 4, the secrecy rules for Defence industry, following from contracts with MoDs, imply that staff working on military projects are not allowed to share knowledge to other departments within the same company**.** This prevents the cross-over of knowledge and thus hampers civil-military synergies.

Chapter 5 pointed out that potential civil-military technology synergies arise through common operational capability requirements and technology needs in both domains. Companies seeking to pursue spin-offs must possess technologies that correspond to the common needs of both sectors. Accordingly, for example, defence companies have no basis to enter the security sector unless they possess technologies that meet the needs of the security sector. For this reason, possessing strong technologies for one sector is an insufficient basis for entering another market. What is required is technology valuable for both sectors. This requires, also, that a company's technology has competitive advantage over that of its competitors. Additionally, a number of other aspects of a technology may require consideration for successful transfer from one sector to another. These include, for example, the extent to which it is compatible with the general environment ('world') of the potential adopter (see section 5.3.1.). Thus, a wide variety of factors affect the role and influence of civil-military (technology) synergies on industry (firm) behaviour and development approaches.

8.4 Assessment of impacts

This section addresses the assessment of the impacts of the different policy options. As such, it combines a quantitative estimate for the potential impact of civil-military synergies for a number of functional areas, with a largely qualitative assessment of the impacts of the different policy options. First, for some selected systems and functional areas a quantitative estimate of the potential impact of civil-military synergies has been made,. Then, for the individual policy options proposed by the Commission a qualitative assessment of the impacts was made. Combining these two pillars then this chapter concludes with a ranking of the these policy options according to how they contribute to maximising civil-military synergies.

The present assessment has largely been based on information obtained from stakeholder interviews, case studies, and a limited number of literature sources, mentioned throughout the text, complemented with a causal chain analysis. In line with the Commission's Guidelines for impact assessment, economic and social impacts are addressed. In this assessment, the impacts are

assessed below, and in the summary table 7.2 economic impacts are marked with an {E} and social impacts with an {S}.
The Guidelines indicate that also environmental impacts should be assessed. However, as these are considered to be minimal and of limited relevance in the context of the study, the environmental aspects have been left out.
The impact assessments are made from the perspective of three main stakeholder groups:

1. industry: the producers of civil security and military products;
2. users: the end users of civil security and military products;
3. society as a whole.

If relevant, a category of other impacts is addressed for impacts that cannot be categorised to the three main stakeholder groups as above.

Key in any impact assessment is that the policy options are compared with a baseline situation. Essentially, the baseline option reflects the current situation and assumes no significant (new) policy intervention. For the analysis of impacts, the baseline is characterised as follows: Synergies continue between civil security and military markets and vice versa as before. The majority of spin-offs go from the defence sector to the civil security sector. The case studies in this report exemplify previous synergies. An initial assessment for five subsectors indicate unused potential of around €2.2 billion of sales between 2010 and 2020 (see also §8.5). European policy on civil-military synergies consists of the continuation of the European Framework Cooperation between the European Defence Agency, the European Commission and the European Space Agency.

8.4.1 Baseline option

In the baseline option, the current situation continues, as addressed above. This implies that civil-military synergies will continue to occur, although it should be mentioned that any insight whether there are annually very many or few civil-military synergies in Europe, or its Member States, is lacking. The case studies presented in Chapter 3 provide a sample of successful spin-offs that occurred in the past without policy intervention. These stem from the initiative of industry (supply-driven synergies) or from market (demand-driven synergies). The civil security R&D and military R&D are also assumed to continue as they have developed in the past few years. The European Commission and the EDA will continue to coordinate their research in the area CBRN protection.

Impact for industry

In section 7.3 lessons from the case studies and interview programme have been reported. Impacts for the military and civil security industry that have been identified include amongst other a decrease of production costs and an increase of sales as a result of continued civil-military synergies at the system and sub-system level. As such, in the baseline, it may be anticipated that additional sales as a result of continued civil-military synergies will continue to occur. .

The current barriers for a further uptake of civil-military synergies continue to exist in the baseline. These barriers are regulation on export control, health, safety and privacy regulation, lack of knowledge of civil markets, a fragmented demand side of the civil security market, an idiosyncratic defence market, and complications with IPR (patenting of technologies used in the defence industry is complicated by the need to disclose potentially sensitive technical information).

Impact for users

The impact for users in the civil security domain is greater availability of systems and subsystems on the market, which could be deployed in the exercise of their tasks. Under condition where these systems and sub-systems represent time-savers, which is supported by e.g. the case studies 1 and

10, users spend more on security equipment but costs are offset by a decrease in personnel and their subsequence costs.

For military users a decrease of procurement costs may be anticipated as a result of an increase of the availability of commercial, off-the-shelf products.

As indicated above, existing barriers for military-civil security synergies, continue to exist and prevent the above impacts from becoming larger.

Impact for society

The expected increase of sales by the civil security and military industry may be accompanied by an increase of demand for production personnel. Hence, overall employment in the civil security and defence industry will increase as well. However, if the additional sales of systems concern systems that allow users to reduce security staff, this will negatively impact employment at end user side.

Additionally, the application of systems and subsystems stemming from civil-military spin-offs by the civil security end users are expected to have a positive impact on their performance, which will lead to an increase of the overall security level in Europe.

The existing barriers for further civil-military synergies prevent further growth of employment in the industry as well as a further increase of the overall security level in Europe.

Other impacts

Another impact that is expected in the baseline option stems from the EFC. The aim of the EFC is to synchronise and complement research activities between the EDA, the European Commission and the ESA and to allow for mutual use of results[147]. Hence synergy between military R&D and civil security R&D is expected as well as reduced duplication of effort in the area to which the EFC now applies – CBRN. However, no barrier within EFC prevents exploring further areas, and the Commission has coordinated its research efforts with the EDA in some specific projects, such as Software Defined Radio..

The next sections deal with more specific policy options, among which is a more structural approach for cooperation under the EFC.

8.4.2 More systematic coordination under EFC

Currently, close cooperation under EFC is hampered by different approaches to R&D activities. The EDA follows a technology approach, while FP7 follows a mission-oriented approach. In other words, the EDA indicates based on a capability analysis what technology is needed to cover a detected capability gap, while FP7 indicates the task to be done, but not the technology to be used.

This policy option takes this difference into account, and aims to bridge the two approaches. As such, the coordination of research activities between FP7 and the EDA through the European Framework Cooperation for Security and Defence continues, as in the baseline, but with an enhancement of EFC in a qualitative and quantitative way:

[147] Source: http://www.eda.europa.eu/Aboutus/Howwedo/Civmil/EFC.

- Qualitative enhancement: from ad-hoc case-by-case coordination to an approach which allows for more systematic coordination and synchronisation, in which project results from either side (EDA or EC) feed those of the other directly;
- Quantitative enhancement: from the existing cooperation between the EC and the EDA in the area of CBRN protection to a larger number of areas and projects.

Regarding the quantitative enhancement, an extension of the EFC scope could be applicable to the following functional areas:

- Sensor systems and sensor information processing (EDA topic ISR Intelligence, Surveillance and Recognition and Maritime Surveillance);
- Command, Control and (secure) Communications (EDA topic Information Management, and CIS, and UAS further than current ATI).

This is based on an earlier analysis on potential subjects for EFC[148], which have been related to the functional areas of this study. An assessment of the political feasibility of this policy option is not addressed in this study.

Impact for industry

Industry participates in the EC's and EDA's research programmes. The qualitative enhancement of the EFC would imply that there is more sharing of research results between projects carried out under the Framework Programme and under EDA's R&T programme. This transfer of knowledge would lead to project outcomes in these research programmes that better reach the programme's objectives compared to the baseline. In other words, the development of technologies, systems and sub-systems improve. As Chapter 5 indicates, a basic condition for companies seeking spin-offs is that they possess technologies that correspond to the needs of the security and defence sector. As such, the probability for a spin-off to be pursued and to become successful increases. This in turn could lead to an increase of sales for the participating industry, but the impact would be minimal if the research is not supplemented with other tools to improve marketing and promotion efforts of companies.

Another impact for industry is the reduction of duplication of effort. By using the project results from the other programme, project consortia do not need to develop the specific knowledge (fully) in their own projects. The effort can thus be applied to other knowledge topics. This impact applies especially for those research projects in which industry obviously participates and which are not fully funded by the EC or the EDA. See below under "other impacts" for a quantification.

Impact for users

There is no direct impact for users. If the policy option leads to an increase of spin-offs, this would mean that users have more systems and subsystems available to purchase to carry out their civil security and defence tasks. Similar to the baseline option (para 7.4.1), procurement costs may increase as users purchase new systems, and may lead to a reduction of security staff and associated costs.

Impact for society

If the policy option leads to an increase of spin-offs, and if users would procure the systems developed as a result of the spin-offs, it may be anticipated that the overall security level increases. Employment levels in the civil security and military industry is expected to increase if more systems

[148] Source: interview EDA

are procured. However, if the additional sales of systems concern systems that allow users to reduce security staff, this will negatively impact employment at end user side.

Other impacts

Reducing duplication of effort, as addressed under the impact for industry, is also applicable to the EDA, its funding Member States, and the EC. After all, the research projects are partly or fully funded by the EDA (via the Member States) and the EC. One of the main aims of the current EFC is to reduce duplication between defence and civilian research so to save resources. In 2009, the EDA funded 38 projects for a total value of €175 million, with an average value of €4.6 million. To date, no evaluation has been on the effects of the EFC. Given the set-up it seems reasonable to assume that indeed resources will be saved. It is however not possible to quantify this. EDA indicates that quantification may become possible if lessons can be drawn when the current project on UAS is completed. EDA indicates that duplication reductions depend on the fact to which extent one is able to indeed exchange research results.

The qualitative and quantitative enhancement of the EFC, i.e. an increase of coordination in a more systematic way, would imply an increase of coordination effort at the EDA and EC. At present, only one person coordinates the EFC at the EDA and one in the EC, which would at least need to double. This is thus an increase of the administrative costs for the Commission and the EDA of approximately €100,000 per year.

8.4.3 Promote hybrid standards

In this option, the Commission takes the lead in formulating and establishing European standards in the functional areas mentioned in this report, and in promoting the use of those standards in both the civil security and military domain. As this policy option is labelled as the *promotion* of hybrid standards, there is no certainty that these hybrid standards will be established and applied.

Currently, the European Committee for Standardisation is already engaged in activities around setting standards for both defence and security, with activities already taking place in the following fields:

- Societal and citizen security (CEN/TC 391);
- Eurocodes (CEN/TC 250);
- Transport of dangerous goods (CEN/TC 296);
- Urban design against crime (CEN/TC 325);
- Humanitarian mine action;
- Defence procurement;
- Co-operation with NSA (expertise in radiological and nuclear detectors, decontamination and modelling, interoperable communications);
- Civil protection (ISO/TC 223, CEN/TC 239);
- Network and Information Security (joint CEN/ISSS and ETSI Focus Group and ISO/IEC JTC 1 'Information technology');
- Biometrics (ISO/IEC JTC 1/ SC 37);
- Certification of equipment and personnel (CEN/CENELEC JTC 1, ISO CASCO);
- Designing crime out of products;
- Marking of small arms.

As has been mentioned in the European Commission communication COM (2008) and in previous report recommendations (Ecorys 2009), quicker and more dynamic standardisation remains a goal,

and this should again be reiterated. In addition, the goal of these (hybrid) standards needs to be on interoperability, and on the technical interoperability standards that will help establish this. While organisational interoperability standards could potentially lead to adoption of certain technical standards, it remains unclear whether anything beyond "best practice" should be pursued at this level.

Technical standards can only be taken so far, as some areas will be more sensitive to trade secrets than others. This should not, however, prevent some level of standardisation. Cryptology provides an instructive example, as for technology areas such as encryption and wireless communication standards have been achieved, despite the sensitivity of the subject.

There is a growing spin-in of civil technologies and components, and therefore of civil standards, into the military market. However, the role of the civil security market as a possible intermediate agent in the transfer of technology between the civil market in general and the military market is very limited. Only a few actual cases come to mind (such as some non-lethal weapons). Standardisation at the technical level is therefore not so much a question of conformity between the civil security and military sector, but rather between the defence and civil domain in general. This falls outside the scope of the study. Standardisation at the organisational level should be based on similarities of missions, tasks and capabilities between the civil security and military domain. Indeed, increasing overlap between 'high-end' civil security and 'low-end' military tasks is evident. A number of tendencies, as described in Chapter 6, could accelerate the process of organisational interoperability standardisation. Harmonisation at the architectural level addresses distributed functionalities that can be linked together in (both physical and logical/functional) networks. These different levels of standardisation are combined to address the impacts per stakeholder below.

It should be pointed out that more stringent European standards could potentially work as a counter to the relative American strength in this area. Comparing the American and European situation, in the United States, the level of government responsible for pressing standards is also the one responsible for procurement decisions. In Europe, on the other hand, the ultimate procurement authority lies at the national level, thus creating possible fragmentation and weakness in standards. The European Directive 2009/81/EC on procurement for the defence and security industries, which is transposed by the various Member States, encourages procurers to use standards, but, exemptions within the Directive still open the possibility of fragmentation. For example, Article 18§3 of the Directive states:

> Without prejudice to either compulsory national technical rules (including those related to product safety) or the technical requirements to be met by the Member State under international standardisation agreements in order to guarantee the interoperability required by those agreements, and provided they are compatible with Community law, technical specifications shall be drawn up.

While Directives are bringing the Member States together, the fact remains that room for fragmentation still exists.

Impacts on industry and users

The security market is fragmented and conservative about untested technologies, which also causes customers in this area to be conservative about new acquisition. This is in direct contrast to the defence industry, in which governments are willing to commit to new technologies in the race to maintain or even increase a technological edge over potential rivals and threats. This difference presents particular problems for military technologies looking to cross-over to the civilian world. Companies developing military products need to be able to provide assurances to civilian

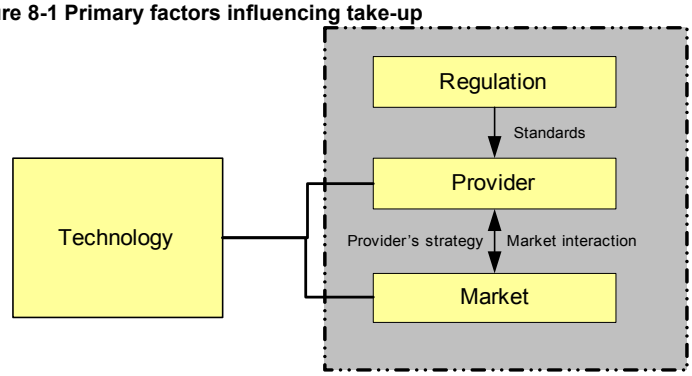
customers that their products are well-tested and ready to fit into existing systems. Hybrid standards would be an added value for that.

Standards can play an important role in increasing buyer confidence that new technologies will not become quickly obsolete and that they can be trusted. On one side, standards reduce the uncertainty of future payoffs, decreasing a potential purchaser's propensity to delay a purchase (Koski & Kretschmer, 2005). On the other side, numerous studies have shown so-called "network effects", with wide product availability influencing uptake of new technologies (Doganoglu & Grzybowski, 2007). If, for example, a civil security agency sees several neighbouring police forces using a command & control system, that agency will be more likely to also adopt that systemwhich has a positive impact on sales for industry.

Measuring the precise impact of these network effects can be extremely difficult. The quantitative studies on network effects that exist, generally focus on establishing the statistical significance of these effects on the demand side (the willingness of an individual to buy) and on the supply side (the willingness to pay more for a product with significant network effects).[149]

At the same time, if governments stand behind particular standards—which would be important in the security and defence industries, given that governments are also some of the main clients for these companies—this further increases the confidence for both producers and purchasers.

Figure 8-1 Primary factors influencing take-up



Source: Adapted from Suryanegara & Miyazaki, 2010.

Standards, however, cannot be seen as a magic bullet to increase adoption of new technologies and smooth the innovation cycle. The current discussion over IPv6—a new internet addressing scheme intended to replace IPv4, the current standard on the Internet—is a good example of the path dependency issue. For more than a decade, experts have been warning that the number of IP addresses, the 12-digit address that are assigned to computers accessing the internet, would be fully allocated. IPv6 resolves this issue by allowing for a far greater number of addresses.[150] First developed in 1995, industry widely agrees that the new IPv6 standard is a good one, but this addressing scheme works differently enough that it would require new hardware across the industry, an expensive and potentially disruptive process, which has caused companies to find innovative ways to work within current limitations rather than jump to the new standard.

The way that standards enter the market, either enforced by the government or adopted by members of industry themselves, also has an influence on the confidence of both producers and customers. Whether these standards are made mandatory, for example, will also influence the level

[149] While modelling these network effects might be possible, they remain outside the bounds of this study.

[150] By one estimate, 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses at the currently suggested 128 bit address scheme.

adoption. Obviously, government mandated standards will have a near immediate impact on adoption of a particular technology, as companies are essentially coerced into adopting a particular standard.

Indeed, government-backed standards are also already working their way into the defence industry. For more than 30 years, the NATO Committee for Standardization has been active in co-ordinating various member activities on issues such as the technical interoperability between communication and information systems. The European Defence Agency is also heavily involved in the standardisation debate, organising workshops and publishing a journal on the subject. In 2011, the EDA published the European Defence Standards Reference System, containing recommendations for 20 different areas.

Common or hybrid standardisation may further facilitate common procurement of systems and subsystems by military and civil security users. Such standards would ease the formulation of the system requirements in the procurement documentation, which would facilitate the bundling of demand which in the end would reduce procurement costs.

These standards, however, face a couple of problems. First, some industries are reticent regarding such standards, as it could potentially mean destroying some of their business models, which are sometimes based on the ability to run a civil security and a defence business unit in the same company dealing with very similar technologies (example SDR).
Second, for all of their work, these standards are—in the end—voluntary and potentially come across one further problem seen in standardisation drives: the adoption of competing standards. Standard settings that are voluntary can lead to conflict. Consortia of companies may line up behind particular standards given their own financial interests. With two (or more) powerful consortia pushing standards, it does little to assuage user fears that they will pick the “wrong” standards, and their investment as an early adopter will be a waste of resources. While procurement directives push the players together to adopt standards, given that national security “remains the sole responsibility of each Member State” (Directive 2009/81/EC), some tensions over standard setting will remain.

Impact for society

While the impact on industry and users is clear, the impact on society is slightly less clear. Greater competitiveness of the industry will, of course, lead to greater employment in the sector and growth. Arguably, greater standards in security would help efforts to create greater interoperability between Member States. Technical standards, for instance, may help to ensure that first-responders can more easily communicate across borders, and a focus on procedural best practice can help to make communication across jurisdictions easier, in cases where this is deemed to be appropriate.

Other impacts

Given the necessity of using discussion to try to achieve consensus on particular standards, there will undoubtedly be additional administrative costs. Companies themselves will also need to increase lobbying efforts, and the risk here is that companies spend more time lobbying for particular standards than innovating.

8.4.4 Establish a High Level Stakeholder Group

One further option is to establish a High Level Stakeholder Group on civ-mil synergies. The aim of this group might be to identify jointly, in a top-down approach, the areas where common research, development or even procurement of products should be initiated and where a common requirement for civil security and military end users could be set.

The exact participation of such High Level Stakeholder Group is not yet defined. Based on the analysis of the cases and the interviews with stakeholders, there are a number of issues in the area of civil military synergies that can be addressed in the Stakeholder group. From this, some stakeholder types follow:

- Common research and development:
  - Requires civil security manufacturers and military manufacturers to attend. To prevent certain interests to prevail over others, one could consider to limit the group to the representing organisations (e.g. ASD and EOS), and invite individual companies on a thematic basis;
  - Requires civil security and military end users to attend to define their needs for common R&D.
- Formulation of requirements for common procurement of systems or subsystems:
  - Requires end users from the civil security and military to attend.
- Standardisation:
  - Requires standardisation experts or representatives of e.g. CEN and other standardisation bodies to attend.
- Ethical issues:
  - Requires to include experts on ethical and societal issues to attend, e.g. multinational NGOs or Member States.

In addition, there could be room to invite observers or experts. The group can establish sub-groups on dedicated themes that require in-depth analysis and advice.

A typical procedure for the establishment of such group is that:

- The European Commission defines the task and mandate of the High Level Stakeholder Group;
- The European Commission defines the rules for membership appointment;
- The European Commission appoints the Chairman of the High level Stakeholder group;

The European Commission and the Chairman identify, invite, and appoint the other members of the Group

Box 8.1 Different tasks and mandates for a high level stakeholder group

A High Level Stakeholder Group is an undefined concept and does vary in its tasks, mandate and governance. Typical previous High Level Stakeholder Groups on an EU level are, for instance, the CARS 21 High Level Group and the High Level Group on the European Aviation Regulatory Framework. CARS 21 was first created in 2005, and after a brief hiatus, relaunched in 2010. Its mandate is to develop “a competitive EU automotive industry and sustainable mobility and growth in 2020 and beyond.”

The High Level Group on the European Aviation Regulatory Framework’s mandate was to:

- develop proposals to simplify the regulatory framework while ensuring that the Community method should be the driving force in regulation;
- to advise on the future evolution of the EASA and Eurocontrol organisations and how the role of industry should develop within the ATM system;
- provide a roadmap for reform and proposals to ensure successful stakeholder involvement.

The High Level Group has delivered its report, which is the result of the work carried out in December 2006-June 2007.

Also at national level, high level stakeholder groups exists. Of particular interest is the current establishment of Topteams to realise nine top sectors in the Netherlands to improve the competitive

position of industry. Each Topteam consists of a personality from the sector, such as a scientist, a representative from an SME and a civil servant from one of the ministries. Each Topteam has developed an action agenda, which needs to be further elaborated by establishing innovation contracts between industry, knowledge institutes and the government, in which parties commit themselves content-wise and financially. An innovation contract consists in turn of different road maps. For each roadmap, another team is responsible for the implementation, again from industry (SMEs and large firms), knowledge institutes, and government.

While impacts for each segment of stakeholders are described below, it should be noted the inherent limitations of a stakeholder group, where consensus-making makes for slow decisions with (potentially) less power. Additionally, as also indicated below, there is only an indirect link between the establishment of a stakeholder group and the eventual sales from more civil-military synergies, as the latter depends on many other factors.

Impact for industry

The current picture is that users at the national, but also at regional or even local level, sometimes define their requirements for systems themselves. As such, the market is heavily fragmented and the industry needs to spend significantly to promote and demonstrate their products to each of the different users to convince them that their product is the right one, and needs to amend its products to comply with the varying requirements. The establishment of a high level stakeholder group *could* contribute to a better formulation of common requirements for systems and subsystem by civil security end users, and thus reduce market fragmentation. This implies a decrease of promotion and product costs for industry to make their products fit for differing user requirements.

Another impact for industry is that the result of the high level stakeholder group's work is a prioritisation of areas that are most promising in the area of common R&D. Common R&D would reduce potential duplication of efforts, but could also stimulate synergies between civil security and military R&D projects. As such, these projects would become more successful, which in turn increases the chance that more spin-offs reach the market, increasing sales. It must be underlined that the link between the establishment of the high level stakeholder group and the eventual additional sales is only an indirect cause-effect relationship. Additional sales depend on many other issues.

If standards are addressed in the high level group, this could eventually lead to more common standards. However, this depends on more issues, and would only be a contributing factor. See the previous section on hybrid standards.

Impact for users

The impact for users as a result of the establishment of a high level stakeholder group is closely related to the impact for industry. The high level stakeholder group would be a yet not-existing platform for civil security users, in which there would be collaboration on the formulation of requirements. This would stimulate the exchange of knowledge between civil security users on available technologies and systems, but would also provide guidance to users that are not at the table of the high level group. In the end, this should lead to procurement of systems and subsystems that are more optimal to the needs of the users.

Additionally, if in the High Level Stakeholder Group, civil security and military users are able to discuss and align the requirements for (certain) civil security and military systems, this could facilitate common procurement processes of those systems for which requirements have been aligned. This could in turn lead to a reduction of procurement costs for civil security and military users.

The definition and prioritisation of common R&D topics could reduce duplication of R&D efforts, which is positive for end users. Additionally, as described above, this stimulates synergies between civil security and military R&D projects. As such, these projects would become more successful, which in turn increases the chance that more spin-offs reach the market. This means that users have more systems and subsystems to carry out their civil security and defence tasks. This could increase procurement costs of these systems but could also decrease security staff costs if the system leads to an automation of tasks. The procurement costs for military end users could slightly decrease as more commercial off-the-shelf products are available.

Impact for society

The impact for society is twofold. First of all, an eventual increase in the uptake of systems that are a spin-off from civil security to military or vice versa would lead to an increase of employment in industry. As said before, the relation between the establishment of a high level stakeholder group and additional sales is only indirect. This is thus also valid for the relation between the establishment of the high level stakeholder group and additional employment.

More importantly, the definition of common R&D needs and common requirements for systems is anticipated to improve the interoperability of systems in the long run, which would in turn lead to be better implementation of joint military and civil security missions, implying an upward effect on security.

Other impacts

The establishment of the High Level Stakeholder Group leads to limited administrative costs. It is assumed that the Commission would remunerate travel and subsistence costs of the members of the group, and provide the secretariat for the Group. An indicative estimate would be:

- Travel and subsistence costs: 15 members * €750 T+C costs per trip * 4 trips per year = €45,000;
- Secretariat: 1 full time equivalent, € 100,000 labour costs;
- Total: approximately € 145,000 costs per year.

8.4.5 Use Article 185 TFEU

Article 185 TFEU, in short, allows the EU to participate in the joint implementation of (parts of) national R&D programmes. Implementing Article 185 TFEU in the Seventh Framework Programme implies that the participating EU Member States integrate their research efforts by defining and committing themselves to a joint research programme, in which the EU promotes the voluntary integration of scientific, managerial, and financial aspects. The EU provides financial support to the joint implementation of the (parts of the) national research programmes involved, based on a joint programme and the setting-up of a dedicated implementation structure.

In the Specific Programmes of the Framework Programme, four potential initiatives under Article 185 TFEU are identified on the basis of the criteria set out in the Seventh Framework Programme:

1. AAL - a joint research programme on 'Ambient Assisted Living';
2. Bonus - a joint research programme in the field of Baltic Sea research;
3. EMRP - a joint research programme in the field of Metrology (the science of measurement);
4. Eurostars - a joint research programme for research-performing SMEs and their partners.

Article 185 has not yet been applied to civil security. In principle, it is applicable to each of the functional areas of this study.

Impact for industry

An important impact for industry is an increase of funding opportunities for R&D dedicated to civil-military technology and system development as a result of the additional financial support provided by the EU. As Chapter 5 indicates, a basic condition for companies seeking spin-offs is that they possess technologies that correspond to the needs of the security and defence sector. As such, the probability for a spin-off to be pursued and to become successful increases. It may thus be expected that this leads to an increase of the number of spin-offs compared to the baseline, but the increase cannot be quantified. This could eventually lead to an increase of sales inside and outside Europe. The joint programming is also expected to decrease market fragmentation, as the programming is done by a subset of EU Member States and the EU. As such, it may be expected that the participating Member States have a vested in interest in the specific topics that are part of the joint research programme, and that relevant end users are involved in programme formulation. As such, it would bring the participating industry closer to end users, and hence market fragmentation might be somewhat reduced, which could positively affect the sales by industry and as well lead to a reduction of promotion costs.

Impact for users

One of the key specificities of this option is that it leads to a joint research programme between a selection of Member States and EU. It is understood that this enables military and civil security end users of different Member States to contribute to the programme though programme formulation and requirement development. This would stimulate dialogue between civil security and military end users both within and between Member States. While the first dialogue is already institutionalised in NATO, for the latter, this is not (fully) the case. This could stimulate cooperation between different civil security end users, and also reduce R&D duplication efforts.

If the number of spin-offs indeed increases compared to the baseline, which may be expected, this could lead to an increase of procurement costs for civil security end users as there are more technologies and systems available that can contribute to the effective operation of their tasks, while the procurement costs for military end users could decrease as more commercial off the shelf products are available. It could also decrease security staff costs, if the system leads to automation of tasks.

Impact for society

The impact for society may be an overall increase of employment as a result of increased sales as a result of spin-offs. However, if the additional sales of systems concern systems that allow users to reduce security staff, this will negatively impact employment at end user side. Additionally, the security level in Europe could increase if the technology and systems hat come on the market indeed contribute to an improved performance of the end users.

Other impacts

One remaining impact is an increase of the administrative costs:

- For the EU: financial contribution to the joint programme and for the associated implementation structure;
- For the participating member states: financial contribution to the joint programme.

But, the joint programming is also expected to reduce duplication of R&D efforts.

8.4.6 *Scoring and summary*

In the above sections, a description of the impacts of the four options compared to the baseline has been provided. Based on expert judgement, the impacts have been scored to indicate the difference between the expected impacts of the options.

As an overall assessment, the option of the deployment of Article 185 will relatively have the most substantial impacts. The option will lead to more available public R&D funding (which is also an administrative cost), which should lead to more spin-offs and extra sales for industry. It is not possible to estimate the absolute increase of extra sales though. The option on the improved EFC also brings significant impacts in the form of reduced duplication and a higher probability for successful spin-offs. The impact of hybrid standards is potentially large; however, the voluntary character on the adoption of the standards makes it yet unsure whether these standards will be adopted and thus if this potential is ever realised. Finally, the option of the High level Stakeholder Group leads to slightly positive impacts, but does not make a direct link to an increase of sales or reduced duplication of effort. As such, it seems more as a no regret option: it favours some of the conditions for improved spin-off potential and does not cost a lot.

This is all summarised in the table 7.2. The table should be read as follows. The second column describes the impact, and the first column indicates if this impact is positive (+) or negative (-) for that stakeholder. The signs in the columns of the policy options present the development of the impact, and thus indicate whether an impact becomes more positive (+) or negative (-) for that stakeholder. As an example: the increase of marketing costs is in itself a negative issue for a stakeholder. In option 2-4 this impacts becomes more positive for the stakeholders (+), i.e. their marketing costs decrease.

Table 8-2 Overview impact of given policy options

	Impact	Option 0 Baseline	Option 1 Improved EFC	Option 2 Hybrid standards	Option 3 High level SH group	Option 4 Article 185
	Industry					
+	Increase R&D expenditure {E}	0				
-	Increase marketing costs {E}	0		+	+	+
+	Increase of sales {E}	0	+	+	0/+	++
+	Increase of R&D success {E}	0	+		0/+	
+	Reduction duplication of R&D efforts {E}	0	+		0/+	
+	Increase of available R&D funding {E}	0				+
+	Reduction market fragmentation {E}	0		+	+	+
	End users					
-	Increase of procurement costs {E}	0	-	-	-/0	-
+	Decrease of procurement costs {E}	0	+	+	0/+	+
+	Improved cooperation between civil security and military end users {S}	0	+	+	+	+
+	Improved cooperation between			+	+	+

	civil security end users {S}					
+	Improved cooperation between military end users {S}					
	Society	**0**				
+	Increase employment {S}	0	+	+	0/+	+
+	Increase security {S}	0	+	+	0/+	+
	Other					
-	Increase admin costs {E}	0	-	-	-	--
+	Reduced duplication of efforts {E}	0	+		0/+	+
	Overall score					
		0	+	+	0/+	++

E = economic impact, S = social impact.

8.5 Quantitative impact assessment of civil-military synergies for some typical areas

One of the ways assessing the impact of civil-military synergies is measuring what happens when we move from the present state of the market, to a future state where civil-military synergies *have reached their optimum scope*.

To do this, one method is to look at some experiences of civil-military synergies, to see what happened, or what could happen given the proper circumstances. We must keep in mind, however, that real life is the result of complex interactions, and that it is not easy to determine what is due to civil-military synergies per se.

On this basis, extrapolations from such examples may provide an idea of how the whole of the civil-military synergies sphere between the military and security industries can be affected.

8.5.1 What the examples show

Neutron tubes

The example of neutron tubes shows how a supplier of a military product (neutron sources for the French nuclear weapon), driven by the necessity to survive and develop when the military market declines, developed civil applications for a modified version of their original product.

This resulted in diversification towards civil markets. Sodern neutron tube sales in 1990 were 100% to the military. This activity which represents 30% of Sodern sales is now in 2010 split half and half between civil and defence markets. The security activity accounts for about 5% of Sodern sales, to which can be added another 10% for industrial applications from the same dual source.

Table 8-3 Evolution of Sodern activity

	Turnover (million €)	Personnel (number)
2005	50	
2008	50	300
2009	55	320
2010	59	330

Civilian applications can be found particularly in mining, cement factories, oil prospection, drug and explosives detection, and baggage and freight screening.

However there are difficulties with airport baggage screening. French regulation does not allow the use of neutron sources if food or cosmetics are involved. This, and other technical problems, have prevented its application to airport baggage screening in France, and thus potentially in other countries.

Table 8-4 Civil-military synergies impact, the case of Neutron tubes and Sodern

Civil-military synergies	Military to civil
Activity	Diversification to civil markets, new products/systems, growth of sales (+100%) and employment
Impact level	Basic component technology enabling detection systems
Benefits	New functions in mining prospection, quality control, risk detection
Barriers	Regulation of nuclear risk

C3

C3 (also known as command, control, communications, computers, and intelligence or C3) is a wholly dual domain. This is a particular field within the data processing and communications sector, centred on a particular application which originated in the military field using civilian technologies. It extends to security for similar needs, functions, equipment and software.

Quantifying the relative share of military and security is difficult, as the systems are more or less the same, and even the personnel involved are the same. The only way to differentiate the two is by the nature of the customer (military or security).

The applications differ however. Border security for example is very similar to military applications, whereas policing or fire-fighting are more decentralised, using less sophisticated equipment.

The customer attitude is also different. The military have ambitious specifications, but they can accept a system that is not perfect at the start, but that will evolve and adapt. The civilian security market, on the other hand, will only accept a system that is perfectly operational from the start.

A third, important, difference is in the field of standards. In the military market, NATO standards are used all over Europe. In the civilian security market there are no standards yet, though an OASIS[151] standard may be emerging for civilian C3. The main question is whether common exchange protocols can be developed.

Much of the work already developed by OASIS is focussed on markup languages based around XML, providing protocols under which different providers can communicate. One such standard, for example, is the Common Alerting Protocol, with its most recent iteration having been approved in July 2010 (SAML). The standards generally focus on a subsystem level, not addressing any particular application or telecommunications method, meaning that the means to secure and authenticate content can differ according to the client's needs.

Thus it would probably be useful to harmonise civilian C3 needs, and maybe to attempt to transpose NATO standards, and to this end to integrate the military into the civilian security work

[151] **OASIS** (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society - http://www.oasis-open.org/org.

groups. This is not done yet at the European level, though some of the firms that are involved in both the defence and security industries do sit on OASIS committees, such as Airbus.

Table 8-5 C3 markets (billion €)

	2010	2020
Military	6.8	2.8
Civil	1.2	5.2
Total	**8.0**	**8.0**

Source: Forecast International, DECISION.

Table 8-6 Civil-military synergies impact, the case of C3

Civil-military synergies	Technologies: civil to military C3 application: military to civil
Activity	New domain, but small segment of global data processing and communications Security markets can represent a significant addition to military markets
Impact level	Services, supplier-customer organisation
Benefits	New functions, more efficient action by military and civil security players
Barriers	Lack of standards in the civil security field Civil-military synergies must be organised to be fully beneficial

UAVs (Unmanned Aerial Vehicles)

The UAV domain comprises several segments, including airframe platform, payload, architecture, command & control and C3. Airframe technology comes mostly from civil aviation, whereas payloads technologies were more developed more by the military. Architecture and command-control systems have been developed equally by both sides.

Table 8-7 European market for UAVs (units)

	Military	Civil	Total
2008	200	<5	200
2010	300	5	305
2012	400	10	410
2020	800	100	900

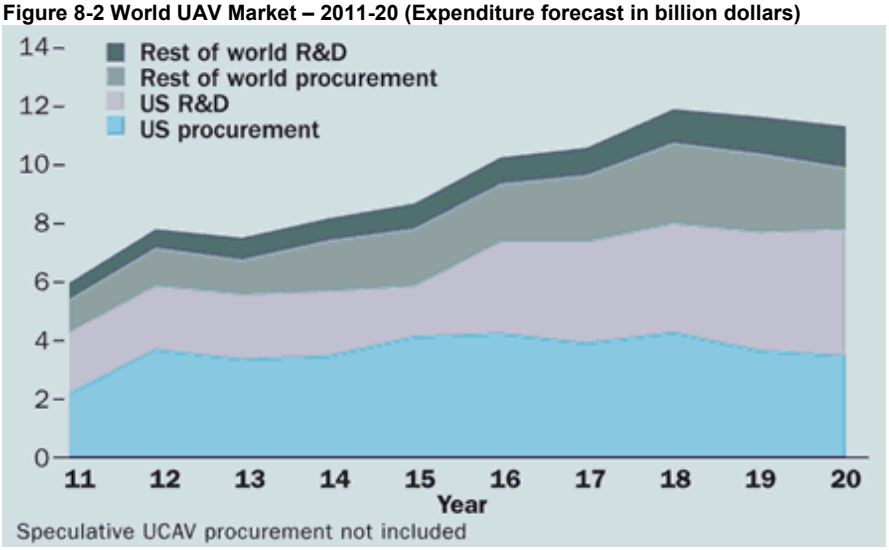
Source: adapted from Frost & Sullivan.

Given that development is already taking place in both civil and military spheres for architecture and communication, it seems that these are the areas that are most ripe for exploitation of synergies. While this report has earlier mentioned that most crossovers flow from the military to the civil side, this is one of the areas where the reverse has been proven to be possible, as shown by the case study on LUNA.

While European armed forces exploit UAVs less than in the US or Israel, the fact that a German firm has managed to achieve a crossover demonstrates that this need not be a barrier. While European industry tends to be less advanced, particularly because without a purely European operational supply in the MALE (Medium Altitude Long Endurance) or HALE (High Altitude Long Endurance) segments, successes are still possible.

More importantly, what this example demonstrates is that in cases where military and civilian needs are relatively close (which is the exception rather than the rule), civilian firms could have an easier time crossing over than military ones. Military clients, as demonstrated earlier, are generally more tolerant of works in progress. The issues that civilian firms will face here is understanding military government acquisition procedures and breaking through the long term relationships between defence industry and MoDs.

Figure 8-2 World UAV Market – 2011-20 (Expenditure forecast in billion dollars)



Source Teal Group.

For UAVs another aspect of civil-military synergies could be the use in some cases by the military of their UAVs for civil uses.

Table 8-8 UAVs world market (million $)

	2011	2020
US procurement	2 200	3 600
Rest of the world procurement	1 200	2 200
Total procurement	**3 400**	**5 800**
US R&D	2 200	4 400
Rest of world R&D	500	1 200
Total R&D	**2 700**	**3 600**

Source Teal Group.

Table 8-9 Civil-military synergies impact, the case of UAVs

Civil-military synergies	Highly dual from the origin Present development is led by military applications No great difference between civil and military needs and technologies
Activity	Opening of civil market will bring new activity, but this is still only potential
Impact level	Components, equipment, services
Benefits	New functions at lesser cost and risk
Barriers	Regulation Certification

Radio-communications

Basically this sector is driven by civil technologies. PMR (Professional Mobile Radio) and CNR (Combat Network Radio) are tailored for specific security or military applications and constraints, but they use technologies developed for the general civil mobile telephony markets, and this will continue in the future.

The specific military need could be no more than 20%, in the total PMR-CNR segment. But this result would need to be organised, with common work on standards and specifications. In particular it will be necessary to consider military needs in the present phase of civil R&D so that the technologies developed can also be used by the military.

Table 8-10 Radio communications world markets (billion €)

	2010	2020
Single station PMR	1.9	2.4
Trunked PMR	6.0	7.5
of which digital	*(2.0)*	*(5.0)*
CNR-LBMTR	2.3	3.8
Total Mobile Radio	**10.2**	**13.7**

Source: Strategy Analytics, DECISION.

After the present peak in military demand due to renewal, the civil security market should be the driver (after 2015).

Table 8-11 Civil-military synergies impact, the case of Radio-communications

Civil-military synergies	Driven by general civil technologies (GSM, UMTS, LTE).
Activity	Market military driven to 2015; Market civil driven from 2015.
Impact level	Increasingly impact on software as PMR-CNR specificity moves into software.
Benefits	Scale effect from using civil technology; R&D optimisation.
Barriers	Military needs must be considered in civil R&D.

Infrared cameras

Infrared cameras were developed by and for the military. Civil markets will have more than doubled the military market by 2020. It is thought that considerable further market development could come if cooled sensor prices could be cut.

Table 8-12 World market for infrared cameras in 2010

	Military	Security	Commercial	Total
		Million €		
Cooled	1 800	100	100	2 000
Uncooled	800	300	600	1 700
Total	**2 600**	**400**	**700**	**3 700**
		000 units		
Uncooled	110	60	120	290

Source FLIR, SIRICA, Yole, Research & Markets, DECISION.

Table 8-13 Infrared camera world market growth to 2020 (million €)

	2010	2015	2020
Cooled	2 000	2 200	2 400
of which military	*(1 800)*	*(1 850)*	*(1 900)*
Uncooled	1 700	2 500	3 700
of which military	*(800)*	*(850)*	*(900)*
Total	**3 700**	**4 700**	**6 100**
of which military	*2 600*	*2 700*	*2 800*

Source FLIR, SIRICA, Yole, Research & Markets, DECISION.

Table 8-14 Civil-military synergies impact, the case of infrared cameras

Civil-military synergies	Military to civil in two technologies.
Activity	New civil markets developed (30%, of which security 10%).
Impact level	Components, equipment/systems, operation.
Benefits	New functions.
Barriers	Export restrictions; Investment to reduce costs.

8.5.2 What is the overall impact

Military-security synergies are a unique type of military-civil synergy, where the synergies are particularly strong because of strong similarities in application, function and need.

The examples we have looked at show several types of impact on the European industry. In the long term, there seem to be cycles where civil and military markets or technologies are alternately the driving force, and, governed by these cycles, markets and activities fluctuate and change. This is particularly the case in radio-communications.

In the shorter term, and looking forward from today, civil-military synergies either open new civil markets to products developed for the military (neutron tubes, infrared cameras, drones), or they enable scale-effect cost reduction by the military using civil technologies (radio-communications), or they enable development of systems that are specific to the security and military fields (C3).

This is of course a very simplified view, focusing on the more immediate economic results measured on levels of activity and employment.

Table 8-15 Military-civil synergy impact on activity in examples studied

Spin-off generates additional civil markets	
Neutron tubes	Market +100%, of which security +33% up to today.
Infrared cameras	Market +>30% of which security +10% up to today.
UAV	Civil market has not taken off yet; +15% by 2020?
Civil-military synergies generates civil markets to relay military programme completion	
Radio-communications	Dual market, uses civil technologies; Civil market growth will relay military market growth after 2015.
C3	New dual market; Military market could drop by 2020, civil market needed to relay growth.

The following table attempts to quantify the examples that we have discussed. It represents the maximum potential of civil-military synergies. These figures are rough estimates, designed to give orders of magnitude rather than precise indications. Moreover the civil markets given are not only security markets, they often include some industrial or commercial applications, or even, in the case of infrared cameras, automotive applications. It was not possible to go into finer detail.

Table 8-16 Annual markets in the 5 sectors covered, 2010-2020. (million €)

	World		Europe	
	2010	2020	2010	2020
Neutron tubes mil	40	40	15	15
Neutron tubes civ	60	120	15	35
Neutron tubes total	***100***	***160***	***30***	***50***
IR cameras mil	2600	2800	530	540
IR cameras civ	1100	3300	220	660
IR cameras total	***3700***	***6100***	***750***	***1200***
C3 mil	5800	3500	1700	1100
C3 civ	1000	4000	300	1200
C3 total	***6800***	***7500***	***2000***	***2300***
UAV mil	3300	5000	680	1050
UAV civ	100	800	20	150
UAV total	***3400***	***5800***	***700***	***1200***
Radio-comms mil	2300	3800	1500	1000
Radio-comms civ	7900	9900	1000	2500
Radio-comms total	***10200***	***13700***	***2500***	***3500***
All examples mil	14040	15140	4425	3705
All examples civ	10160	18120	1555	4545
All examples total	**24200**	**33260**	**5980**	**8250**

Source: various sources (see above) and DECISION estimates.

At this stage we considered that all market growth up to 2020 could be ascribed to the benefits of civil-military synergies. This is of course only partly true, as there could be some growth from a market size increase in the absence of any civil-military synergies. However, in the examples chosen, civil-military synergies are at the heart of growth through spin-offs generating new markets (in these cases mostly civil, but also military in the case of radio-communications).

Table 8-17 Impact on sales and employment in Europe

	Sales added 2010-2020 (million €)	Of which civil	Employment added (total number)*
Neutron tubes	+20	+20	120
IR cameras	+450	+440	2800
C3	+300	+900	1900
UAV	+500	+130	3100
Radio communications	+1000	+1500	6200
Total	**+2270**	**+1990**	**14120**

*assuming 160 000 € sales per employee, (military and civil sales).

For the five examples studied, the impact on employment in Europe over the next ten years can be evaluated at nearly 15 000 new jobs in the Defence and Security industries and 15 000 more new jobs in equipment-related services. In reality part of this increase will come from sales to other sectors than Defence and Security.

Achieving this result will already require some effort to facilitate diffusion of spin-offs. Additional European policies implemented to increase synergies, in particular through R&D funding, by implementing procedures such as PCP to improve R&D efficiency, or by facilitating organisational means (cooperation between the military and civil prescribers, procurers and users on standards, specifications, regulation, certification, SME policy) to enable civil-military synergies to diffuse more efficiently, could add a twofold effect.

Such policies could accelerate the cross-diffusion of technologies between the military and civil security fields (and sometimes also the commercial field). And they could at the same time strengthen the position of European suppliers and industry on the world markets. Both these effects are cumulative and would increase the positive impact on sales and employment of military-civil synergies.

The examples considered only represent a small part of the security and military markets (around 5%). However, only these five examples of synergies and market growth with no additional action should bring an increase in employment, not counting services, of nearly 3% by 2020.

8.6 Overall assessment

In this section an overall assessment is provided, based on the analysis above. Four scoring criteria have been identified:

- The degree that the policy option tackles existing barriers for spin-offs;
- The overall impact of the option vis-à-vis the baseline, which is the end scores presented in summary table 7.2 ;
- The number of functional areas from the study that are addressed by the option;
- The extent to which the option is estimated to realise the maximum potential of civil-military synergies, as presented in §8.5.

The overall assessment is provided in the table below.

Table 8-18 Overall assessment

		Option 0	Option 1	Option 2	Option 3	Option 4
		Baseline	Improved EFC	Hybrid standards	High level SH group	Article 185
	Tackling existing barriers	0	0	+	+	0
	Overall impact vis-à-vis baseline	0	+	+	0/+	++
	Addressing nr of functional areas	10	2	6	10	10
	Realisation of max potential of civ-mil synergies	0	+	0/+	0/+	++
	Overall score	**0**	**+**	**++**	**+**	**+++**

Two of the policy options directly address existing barriers for spin-offs, which have been described in §7.3. Option 2 on promoting hybrid standards addresses the current barrier on lack of standards, while option 3 High level Stakeholder Group is expected to reduce civil security market fragmentation. The options on an improved EFC and Article 185 do not seem to tackle existing barriers.

The overall impact score has been explained in §7.4.6. The option on Article 185 scores relatively best, while the option on the High level Stakeholder Group is ranked relatively lowest. All options score better than the baseline. It should be noted that also in the baseline it is expected that there will be more civil-military synergies and that these will lead to additional sales for industry.

The options on the High level Stakeholder Group and Article 185 seem in principle be suitable for all 10 functional areas. The option on hybrid standards is most suited for six functional areas (Infrared cameras, C3, Radio Communication, Biometrics, Cyber security, Non-lethal weapons), while the option on the improved EFC is most applicable to two functional areas (Sensor systems and sensor information processing and Command, Control and (secure) Communications).

Finally, the contribution of the options to the maximum potential of civil-military synergies is assessed. This is done by taking into account the largest potential for additional sales of industry as a result of an increase of spin-offs. For the option “Improved EFC” it is expected that the research result improve, and hence the probability of spin-offs realised and being put on the market increases. However, the option is only applicable to a relatively low number of areas. The option to promote hybrid standards addresses the current lack of standards on civil security side, which can improve market uptake. However, the true adoption of standards as a result of this option is uncertain, due to the voluntary character of the option regarding standards adoption. Also, standardisation at the technical level is not so much a question of conformity between the military and civil security, but rather between defence and the civil domain in general. The option of the High Level Stakeholder Group would improve the conditions for industry to increase sales as a result of spin-off. However, the direct relation between the option and increase of sales is limited. Finally, Article 185 would increase R&D efforts in in principle all 10 functional areas. It may be anticipated that this would lead to an increase of spin-offs and thus increase of sales. As such, it is considered to contribute most to the criterion to realise a part of the maximum potential of spin-offs.

The overall conclusion is that the option on article 185 has the best score relative to the other options. However, it would also bring the highest cost as it requires extra R&D funding. The other three options seem ‘no-regret’ options. Costs are fairly limited, while each of them leads to positive impacts in terms of reduced duplication of efforts, increased sales, improved cooperation etc.

9 Conclusions and Recommendations

Conclusions and recommendations listed in this Chapter are based on the analysis done by the project team and do not represent views of the Commission or in any way binding the Commission.

9.1 Observations on the current state of defence - civil security synergies

Conclusion 1. There is a clear rationale and opportunity for exploiting synergies between the military and civil security domains.

Public expenditure in general and on Defence and Security in Europe will be increasingly restricted. At the same time, developments in the security environment lead to increased overlap between the military and civil security domains and a blurred distinction between the two. In this context, there is a clear rationale and opportunity for developing and exploiting synergies between the military and civil security domains, and to strongly promote convergence between the two corresponding industries (see Chapter 1).

Conclusion 2.The defence and civil security domains differ significantly.

The defence and civil security domains differ significantly in the following aspects (see Chapters 1, 3 and 5):

- Demand side: consolidated and public for defence, fragmented and public and private for civil security;
- Supply side: clearly demarcated for defence, blurred for civil security;
- Interaction between demand and supply: well-structured and centralized for defence, decentralized and locally structured in security;
- Technology and product development: longer term technology roadmaps and cost and risk sharing drive innovation for defence, little dedicated innovation for security.

These differences render spin-offs between the two markets difficult. However, realizing the full potential of synergies and complementarities can be a powerful way to maintain, consolidate, and develop the two industries and markets in Europe.

Conclusion 3. Many spin-offs exist between the defence sector and the civil sector in general.

There is substantial flow of spin-offs between the defence sector and the civil sector in general. As technological leadership in many areas formerly dominated by defence R&D shifts to commercial industries we observe a growing use of civil technology and COTS products in military applications. This is backed by formal policy of many European MoDs to make more and better use of 'off-the-shelf' technologies and products. Vice versa, many defence research organizations are now directly charged with the broader commercialization of existing defence technologies in the civil domain (including, but not confined to, the civil security domain). However, the project team did not look specifically at these broader spin-offs and related issues as they lie **outside the Terms of Reference** of the project (see Chapters 1, 3 and 5).

Conclusion 4. Relatively few products are deliberately designed for both markets from the outset (preconceived spin-offs). Most spin-offs run from defence to civil security.

The case studies (Chapter 3) show that, up to now, preconceived spin-offs between the defence and the civil security market, or products that were deliberately designed and developed for both military and civil security market are relatively scarce. Although it is difficult to be confident without extensive access to internal companies' documents, many of the spin-off cases appear to be opportunistic rather than purposefully planned up-front.

Pressured by declining defence budgets in Europe and encouraged by high importance of civil security on the political agenda in the wake of '9/11' and other terroristic incidents, many European defence companies saw opportunities to expand their business to the emerging security market. Their solid technological base established through defence R&D was viewed as the fundament for business development in the security sector. However, the clear distinction between the two markets, as described in Chapter 1, rendered the exploitation of synergies and the resulting spin-offs difficult. Products developed for the defence sector tend to be over-specified and too expensive for the security sector. In addition, the marketing capabilities required for success in the defence market differ significantly from those needed to have success in the security sector. In the defence sector, relational capital build up over years working with single MoDs is paramount for product development in conformity to set requirements. This is quite different from doing business in the fragmented, cost-driven security sector. These differences seem to have been underestimated by a number of well-known defence companies. In particular, the need to invest in non-technological capabilities, such as marketing, for succeeding in the new markets was not sufficiently appreciated. And indeed, where traditional defence companies have developed a civil security portfolio, the two segments are run in separate business units, with largely separated business logic, R&D etc. In short, synergies between the defence and security domains appeared to be less obvious and more difficult to achieve than many defence companies initially hoped for.

In addition, defence companies perceive a risk that if they more actively (and successfully) pursue spin-offs, governments might respond by building-in assumptions about 'spin-off potential' into defence sector R&D funding. In essence, this would amount to a mechanism for transferring risk from the government to the defence contractors. So for the defence sector, part of the cost-benefit equation for pursuing spin-offs is the trade-off between the possible future additional revenues and the possible future negative impacts on R&D funding levels and risks. Comparing the defence sector with the commercial sector, in the defence sector successful spin-offs would be an argument for governments to cut R&D funding while for the commercial sector successful spin-offs are an argument to increase R&D funding (Chapter 5).

Furthermore, we have found that almost all spin-offs run from the defence to the civil security market. Spin-offs in the opposite direction, from civil security to defence, appear to be very limited in number and scope. The main reason for this imbalance is that the established defence sector has a much higher R&D expenditure than the quite fragmented and relatively young civil security sector. Governments typically are more ready to cover private R&D costs in the defence than in the civil security domain (Chapters 3 and 5).

9.2 Opportunities for (increased) future synergies

Conclusion 5. Overlap in 'low end' military and 'high end' civil security missions provides opportunities for synergy.

The overlap in missions (e.g. border control) and tasks (e.g. surveillance and intelligence) provides a strong and immediate potential for 'bridging' technologies, products and services that can be applied in both markets (see Chapter 1, 3 and 5).

Conclusion 6. Defence budget cuts create more pressure to exploit synergies.

The current and likely future budget cuts in this era of austerity, put emphasis on cost reduction and 'value for money' considerations in the defence domain. Economies of scale and the possibility of sharing non-recurrent costs such as R&D is important. In a shrinking market, defence companies again are looking at 'adjacent' markets, such as the civil security market, to achieve economies of scale.

By assimilating lessons learned from past experience, developing and exploiting synergies should prove to be more successful than before. With the progressive decline of military budgets and the structural weakness of security budgets, industry is very much aware that an increased synergy between military and civil security technologies is an important, and in some cases a necessary, condition for a sustainable business. This is in particular true in areas such as unmanned aerial systems, C3, and personal protection. Modular approaches in both design and production processes, aimed at flexible products coming from the same industrial and technological base, as well as organising convergence from the start between all stakeholders, is the key to success (see Chapters 1 and 5).

Conclusion 7. Such areas as cyber security, sensor systems and C3 provide significant potential for future synergies.

In spite of practical difficulties, ultimately the increased ability to respond to market needs, the potential for more sales, market coverage and employment, and reduced overhead costs and risks that would stem from increased synergies, is seen as a positive outcome by all players and stakeholders (Chapter 5). In particular, there is substantial potential for market growth in the areas where overlap in missions or enabling technologies or both between the defence and civil security domains exists. Analysis of the identified spin-off cases show that most have occurred in the areas of sensor systems and command, control and communications (C3). Results from an expert assessment of the functional areas with the largest potential for synergies suggest that cyber security has probably the largest potential for synergies, followed by sensor systems (including information processing). Given that C3 and cyber security are closely related, we conclude that sensors and C3 systems (with the inclusion of information processing and IT security) are the two functional areas that best combine market size and expected growth with synergetic potential in terms of shared technologies, R&D and possibly products and services (see Chapter 4).

Conclusion 8. Structural barriers need to be addressed to facilitate more and more successful synergies.

The most important structural barriers that hamper synergies between the defence and civil security market, and therefore need to be addressed by possible policy options, are (see Chapters 3 and 5):

1. Lack of (consolidated) longer term visions and technology roadmaps in the civil security domain to guide the market and warrant investments on both the demand and supply side;
2. High entrance costs from defence to civil security market, associated with the transition from technology development to placing a product on the market; as well as with securing the market (e.g. lobbying, marketing, commercial diplomacy). The (perceived) threat of reduced government funding for defence R&D if defence companies create successful spin-off in the civil market (including civil security), could be considered as part of the entrance costs;
3. Regulation on export control, as well as on comfort, health, safety and privacy issues;
4. Sensitivity and classification of defence technologies, leading to severe limitations to use these technologies outside of a strict (national) defence domain.

Conclusion 9. National initiatives under way to create more structure in the civil security sector.

One of the main barriers for creating synergies between the defence and the civil security domain is the lack of a longer term perspective in the civil security domain. Development of such a perspective should go hand in hand with a process of consolidation, where a longer term vision can be both the result of and a trigger for consolidation.

Some Member States have recognized the value of longer term planning in the security domain and have started a process of developing some sort of "capability based planning" approach, similar to the one cultivated in the military domain over many years. In addition, these MS have started comparing military and security capacity development plans and are looking for shared road maps to delineate dual technology needs. These sort of efforts can be seen, amongst others, in France, the United Kingdom and the Netherlands.[152] Such national initiatives on military-civil security synergies indicate that, despite obvious difficulties, conditions exist for implementing a meaningful policy reform in the field. If and where possible, policy measures at the EU-level should take into account and build upon these national initiatives.

Recommendation 1. To foster military – civil security synergies the European Commission could promote best practices with respect to a 'capability based approach' for civil security amongst the MSs, building upon various national initiatives already under way. This should lead to a process of establishing shared defence-security technology and capability road maps and, eventually, joint R&D efforts to implement these roadmaps.

[152] For example, National Security through Technology: Technology, Equipment, and Support for UK Defence and Security (Cm 8278), February 2012.

9.3 Policy options and their impact

Conclusion 10. The policy option 'Improved EFC' is a 'no-regret' option, but doesn't directly address the structural barriers.

Moving from a case by case and ad hoc cooperation to a systematic synchronisation between research projects of the Commission and of the EDA could be achieved with little or no additional cost and therefore can be seen as 'no-regret' option. The biggest challenge would be to achieve integration while doing justice to the respective responsibilities and decision structures of the two sides involved. However, EFC remains oriented towards individual projects. While this policy option will strengthen the efficiency and applicability of these projects, which could increase the probability of incidental synergies as a result, it does not directly address the structural barriers for more and more successful synergies between the defence and civil security markets (see Chapters 6 and 7).

Recommendation 2. The European Commission could look at ways to use EFC to promote the establishment and implementation of shared defence-security technology and capability road maps.

Conclusion 11

a. The policy option 'Promote hybrid standards', when applied at the technical level, should be aimed at the interaction between defence and civil standards in general;

b. The policy option 'Promote hybrid standards' when applied at the organisational and architectural level, may help to address some structural barriers.

Standardisation at the technical level (including technical interoperability standards and common performance standards) in general does lead to increased buyer confidence and a more rapid dissemination of technologies, with a positive impact on sales for industry. However, standardisation at the technical level is not so much a question of conformity between the military and civil security, but rather between the defence and the civil domain in general. This falls outside the scope of this study.

Standardisation or harmonization at the organisational level based on similarities of missions, tasks and capabilities between the civil security and military domain, could stimulate synergies. Organisational interoperability standards focus on protocols, procedures and guidelines to ensure interoperability. In addition to organisational interoperability standards sharing best practices (including architectural approaches in developing complex systems) between the two domains is essential. It will stimulate conformity between the two domains at the level of capabilities. This is where the security domain can learn from the longer term approach and perspective that is customary in the defence domain and start developing its own 'capability based approach'. This may help to overcome a fundamental difference between the two domains, thereby facilitating synergies (see Chapters 6 and 7).

Recommendation 3. The European Commission could look at ways to promote best practices and technical / organisational interoperability standards as a solid basis for and element of the process of establishing shared defence-security technology and capability road maps.

Conclusion 12. The policy option 'Article 185' may help to address some structural barriers, in particular to further stimulate national initiatives already under way. The potential additional R&D-funding associated with this option could facilitate an increase of synergies.

'Article 185' is a useful instrument for joint R&D programming of the Commission and a selection of Member States. As such, this option facilitates a dialogue on R&D programming between civil security and military end users nationally, but also between civil security end users across MS. This would contribute to consolidation of the demand side in the civil security sector. In particular, this option should be seen as a way to stimulate national initiatives already under way in a number of Member States, as described in Conclusion 8.

Assuming that the application of Article 185 in the civil security – military research domain would imply (additional) financial support by the EU, R&D funding availability thus increases for this area, thereby facilitating synergies (see Chapters 6 and 7).

Recommendation 4. The European Commission could have the use of 'Article 185' established as an instrument to bring together interested MSs for joint R&D efforts as part of shared defence-security technology and capability road maps.

Conclusion 13. The policy option 'create a high level stakeholder group' doesn't directly address the structural barriers, but may create conditions for other favourable initiatives to succeed.

A high-level stakeholder group could be instrumental in creating better conditions for possible future synergies, rather than in directly facilitating synergies. Examples of such conditions include more aligned requirements in the civil security market (less fragmentation); and stimuli to coordinate research by the EC (with a civil security angle) and the EDA (with a defence angle) that could lead to a reduced duplication of efforts and/or alignment of technology developments and innovation in the two domains (see Chapters 6 and 7).

Recommendation 5. The European Commission could reflect on establishing a high level stake holder group as a way to create more favourable conditions for and stakeholder 'buying-in' of implementing the other recommendations.

Conclusion 14. Other policy options need to be considered to address the structural barriers; some of these lying outside the scope of the Commission.

The proposed policy options only partially address the structural barriers for increased synergies, as identified in Conclusion 9. The first barrier, the lack of longer term visions and technology roadmaps in the civil security sector, primarily lies at a national level. Indeed, a number of national initiatives are under way to address that barrier. The Commission could coordinate with the Member States that have already launched concrete initiatives, for example by facilitating exchange of best practices and lessons learned. The Commission may also take the lead in initiatives that

would stimulate a 'Capability Based Planning' approach for civil security mission areas where the EU has political and operational responsibilities, such as FRONTEX.

The second barrier, the high entrance costs from the defence to the civil security market, is not so much a matter of high costs per se, but rather of the balance between (up front) market entrance costs versus (future) new market revenues. It is industry itself that may lower the entrance costs, e.g. by modular approaches in design and production processes, aimed at flexible products coming from the same industrial and technological base and serving both markets. National governments can also facilitate, e.g. by not punishing spin-off successes by cutting down on defence R&D. The role of the Commission in this areas seems to be limited.

The third barrier, regulation, lies both at the national and at the EU level. Overcoming this barrier by revisiting existing regulation will probably have to be done on a case by case basis. The Commission could play an important role in overcoming this barrier by revisiting existing regulation, but we haven't looked into the matter.

The fourth barrier, classification issues that prevent the sharing of know-how and technologies, also require a case by case approach. As far as public interests are concerned, this approach seems to lie more at a national level then at an EU-level (the commercial interests involved lie with industry itself).

Recommendation 6. Next to stimulating national initiatives already under way (recommendation 1), the European Commission could explore the possibility of establishing shared defence-security technology and capability road maps for mission areas for which the EU has political and operational responsibilities, such as FRONTEX.

Annex 1 Sources

ASD, Facts and Figures 2010.

Bailes, A. J., and S. Depauw, *The EU Defence Market: Balancing Effectiveness with Responsibility*. Available at http://www.sipri.org/research/armaments/transfers/publications/other_publ/other%20publications/conference-report-eu-defence-market-flemish-peace-institute.

Bolkcom C. and B. Elias, "*Homeland Security: Protecting Airliners From Terrorist Missiles*," CRS Report for Congress, RL31741, February 16, 2006.

Brzoska Michael, "Trends in Global Military and Civilian Research and Development and their Changing Interface", in: Proceedings of the International Seminar on Defence Finance and Economics, 13-15 November 2006, New Delhi, India 2006, S. 289-302

Chait R., A. Sciarretta, and D. Shorts, *Army Science and Technology Analysis for Stabilization and Reconstruction Operations*, Center for Technology and National Security Policy, October 2006.

Centre for Strategy and Evaluation Services, Ex-post evaluation of PASR and interim evaluation of FP7 security research, 2011.

Defence Science Board (DSB), *Buying Commercial: Gaining the Cost/Schedule Benefits for Defence Systems*, February 2009, available at http://www.acq.osd.mil/dsb/reports/ADA494760.pdf (as of December 20, 2 011).

Doganoglu, T. and L. Grzybowski, Estimating Network Effects in Mobile Telephony in Germany. *Information Economics and Policy*, 19(1), 2007, 65–79.

Drent, M., and D. Zandee, *Breaking Pillars. Towards a Civil-Military Security Approach for the European Union*, Clingendael, January 2010, available at http://www.clingendael.nl/publications/2010/20100211_breaking_pillars.pdf.

ECORYS, DECISION and TNO, *Study on the Competitiveness of the EU security industry*, 15 November 2009, study commissioned by DG Enterprise & Industry.

European Commission, *Research for a Secure Europe- Report of the Group of Personalities in the field of Security Research,* 2003, available at http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf.

European Commission Communication, *"An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and sustainability at Centre Stage,"* Brussels, COM(2010) 614.

European Commission, *Public Consultation on the preparation of a new Communication on an Industrial Policy for the Security Industry*, 2011, available at http://ec.europa.eu/enterprise/policies/security/files/doc/public_consultation/background_document_en.pdf.

European Security Research Advisory Board (ESRAB*), Meeting the Challenge: European Security Research Agenda*, 2006, available at http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf.

European Security Research and Innovation Forum (ESRIF), ESRIF Final Report, 2009, available at: http://www.gppq.mctes.pt/brochuras/online/ESRIF_Final%20report_2009.pdf.

FRANCE. Présidence de la République; FRANCE. Ministère de la défense; MALLET, Jean-Claude, *'Défense et la sécurité nationale: le livre blanc'*, Ed. Odile Jacob : La Documentation française, June 2008.

HM Government*, Securing Britain in an Age of Uncertainty: Strategic Defence and Security Review*, 2010.

HM Government, *National Security Through Technology: Technology, Equipment and Support for UK Defence and Security*, 2012.

IDC, *The European Network and Information Security Market. Scenario, Trend and Challenges*. A Study for the European Commission, DG Information Society and Media. Brussels, 2009.

Istituto Affari Internazionali (IAI), IRIS and Manchester Institute for Innovation Research, *Study on the industrial implications in Europe of the blurring of dividing lines between security and defence*, 2010, study commissioned by DG Enterprise & Industry. Available at http://ec.europa.eu/enterprise/sectors/defence/files/new_defsec_final_report_en.pdf.

James, A., *Defence and Security R&D in Europe*. SANDERA Background Paper, 2009, available at http://www.sandera.net/.

James, A., *SANDERA: The Future of Security and Defence Policies in the European Research Area*. Retrieved December 13, 2011, available at http://www.sandera.net/.

Koski, H., and T. Kretschmer, Innovation and Dominant Design in Mobile Telephony. *Industry & Innovation*, 14(3), 2007, pp.305–324.

Lavallée, C., The European Commission's Position in the Field of Security and Defence: An Unconventional Actor at a Meeting Point*. Perspectives on European Politics and Society*, 12(4), 2011.

Lorell, Mark A., Julia F. Lowell, Michael Kennedy and Hugh P. Levaux, *Cheaper, Faster, Better? Commercial Approaches to Weapons Acquisition,* Santa Monica, Calif: RAND Corporation, MR-1147-AF, 2000. Available at http://www.rand.org/pubs/monograph_reports/MR1147.

Manchester Institute of Innovation Research and Centre for Defence Economics, *Study on How to measure Strengths and Weaknesses of the DTIB in Europe*, 2008, study commissioned by the EDA.

Masson Hélène and Lucia Marta, "The Security Market in the EU and the United States: Features and Trends", in the *EU-U.S. Security Strategies: Comparative Scenario and Recommendations*, 2011, available at http://csis.org/files/publication/110614_Conley_EUUSSecurity_WEB.pdf

National Research Council (NRC), *Assessment of the practicality of pulsed fast neutron analysis for aviation security: Summary*, National Academic Press. Washington D.C., 2002a.

National Research Council (NRC), *Making the Nation Safer. The role of Science and Technology in Countering Terrorism*. National Academic Press. Washington D.C., 2002b.

National Research Council (NRC), *Equipping Tomorrow's Military Force: Integration of Commercial and Military Manufacturing in 2010 and Beyon*d, National Academy Press, Washington DC, 2002c, http://www.nap.edu/catalog/10336.html.

National Research Council (NRC), *Science and Technology for Army Homeland Security: Report 1,* National Academy Press, Washington DC, 2003.

NATO, Financial and economic data related to NATO defence, 2011.

Office of Technology Assessment (OTA), *Assessing the Potential for Civil-Military Integration: Technologies, Processes, and Practices*, September 1994, OTA-ISS-611.

Sempere C.M, *Economics of Security Working Paper 43: A survey of the European security market*, Economics of Security Working Paper 43, February 2011.

STAkeholders platform for supply Chain mapping, market Condition Analysis and Technologies Opportunities (STACCATO), Deliverable D 1.2.2. STACCATO Final Taxonomy, 2008, supporting activity within the Preparatory Action on the enhancement of the European industrial potential in the field of Security research (PASR).

TNO, *Development of a European Defence Technological and Industrial Base*, 2009, study commissioned by DG Enterprise & Industry.

U.S. Department of Defence, *Commercial Item Acquisition: Considerations and Lessons Learned*, June 26, 2000, http://www.acq.osd.mil/dpap/Docs/cotsreport.pdf.

U.S. Department of Defence, Military and Security Developments Involving the People's Republic of China. 2010.

U.S. Department of State, *"The MANPADS Menace: Combating the Threat to Global Aviation From Man-Portable Air Defense Systems,"* September 20, 2005 (fact sheet).

Annex 2 List of Acronyms

ASD	Aerospace and Defence Industries Association of Europe
BDSV	Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (Federal Association of German Security and Defence Industry)
BWB	Bundesamt für Wehrtechnik und Beschaffung (Federal Office for Defence Technology and Procurement)
CBRN	Chemical, Biological, Radiological and Nuclear
COTS	Commercial off-the-shelf
CSF	Common Strategic Framework
C3SR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
EC	European Commission
EDA	European Defence Agency
EFC	European Framework Cooperation for Security and Defence
EOS	European Organisation for Security
ESA	European Space Agency
ESD	European Security Directory
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
EU	European Union
FP	Framework Programme
ISIC	International Standard of Industrial Classification
IPR	Intellectual Property Rights
MoD	Ministry of Defence
MoI	Ministry of Interior
NACE	Statistical Classification of Economic Activities in the European Community
NAMSA	NATO Maintenance and Supply Agency
NATO	North Atlantic Treaty Organization
R&D	Research and Development
R&T	Research and Technology
SDR	software defined radio
STACCATO	STAkeholdersplatform for supply Chain mapping, market Condition Analysis and Technologies Opportunities
ToR	Terms of Reference
UAV	Unmanned aerial vehicle
UUV	Unmanned underwater vehicle
WEAG	Western European Armaments Group
WMD	Weapons of mass destruction
WP	Work package

P.O. Box 4175
3006 AD Rotterdam
The Netherlands

Watermanweg 44
3067 GG Rotterdam
The Netherlands

T +31 (0)10 453 88 00
F +31 (0)10 453 07 68
E netherlands@ecorys.com

W www.ecorys.nl

Sound analysis, inspiring ideas