

***Framework Service Contract for the Procurement of
Studies and other Supporting Services on Commission
Impact Assessments and Evaluations***

***Ex-post Evaluation of the
Preparatory Action on Security
Research (PASR)***

***Interim Evaluation of FP7 Security
Research***

Final report (Appendices)

January 2011



**Centre for
Strategy & Evaluation
Services**

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk

Contents

APPENDICES	PAGE
A. List of interviews	110
B. Bibliography	117
C. Interview checklists	120
D. Selection of EU Security projects	130
E. Indicators paper	134
F. Full survey results	135
G. National security research programmes	158
H. Case studies	172
I. Standardisation	173
J. Future perspectives	176

List of interviews

A

No.	Type of interviewee	Name	Organisation	Role/ Position/ Unit
1	Commission official	Tristan SIMONART	DG ENTR	Evaluation project officer
2	Commission official	Ignacio MONTIEL-SANCHEZ	DG ENTR	Security Research Unit, H3
3	Commission official	Paolo Salieri	DG ENTR	Security Research Unit, H3, Maritime Security
4	Commission official	Eva-Maria Engdhal	DG ENTR	Security Research Unit, H3 Society and Ethics
5	Commission official	Christoph Kautz	DG ENTR	Security Research Unit, H3, Deputy Head of Unit
6	Commission official	Ngandu Mupangila	DG ENTR	Security Research Unit, H3, policy official
7	Commission official	Clément Williamson	DG ENTR	Security Research Unit, H3, Project Officer, CBRN
8	Commission official	Khoen van Liehm	DG ENTR	Security Research Unit, H3, Project Officer, aviation security
9	REA official	Christiane Bernard	REA	Head of Security Unit S3
10	REA official	Angelo Marino	REA	Head of Security Unit S3
11	REA official	Andrej Grebenc	REA	Security Unit S3, Technical Project Officer
12	REA official	Alexandros Bakalacos	REA	Security Unit S3, Technical Project Officer
13	REA official	Juliane Giordani	REA	Security Unit S3, Technical Project Officer
14	REA official	Massimo Ciscato	REA	Security Unit S3, Technical Project Officer
15	REA official	Bruno Mastantuono	REA	Security Unit S3, Legal Officer
16	REA official	Pedro de Carvalho	REA	Security Unit S3, Financial Officer
17	Commission official - policy user	Mireille Doerr	DG MOVE	Aviation Security Unit, research and technology
18	Commission official - policy user	Doris Schröcker	DG MOVE	Single Sky & Modernisation of Air Traffic Control
19	Commission official - policy user	Olivier Waldner	DG MOVE	ATM security and in-flight security
20	Commission official - policy user	Caroline Hager	DG JLS	EMCDDA Desk Officer and Programme Coordination Unit D.3. Anti-Drugs Policy
21	Commission official - policy user	Michel Hugon	DG Research, Energy (Euratom)	Unit J-2 Fission CBRN / Euratom (formerly involved in initial preparations for PASR)
22	Commission official - policy user	Patrick Dietz	DG JLS	Counter-terrorism and CBRN detection
23	Commission official - policy user	Christian KRASSNIG	DG JLS	Policy official, counter-terrorism and CBRN detection
24	Commission official - policy user	Jana Paskajova	DG ENTR	Policy official, Crisis management

List of interviews

A

25	Commission official - policy user	Paolo Guglielmetti	DG SANCO	CBRN – health aspects (e.g. protective clothing, treatment of victims of CBRN attacks)
26	MEP – policy user	Jacqueline Foster	European Parliament	Head of Committee on Transport and Tourism

List of interviews

A

No.	Type of Interviewee	Project(s)	Country	Organisation	Name
1	Beneficiary	ADABTS	Sweden	Swedish Defense Research Agency (FOI)	Jörgen Ahlberg
2	Beneficiary	ADABTS	Norway	Detec A/S	Knut Helgsen
3	Beneficiary	AMASS	Czech Rep	HSF	Tomas Metz
4	Beneficiary	AMASS	Germany	Carl Zeiss Optronics	Thomas Anderson
5	Beneficiary	ASTRO+	France	EADS Astrium Grounds Systems	Bruno Vatan
6	Beneficiary	BeSeCu	UK	Behaviour Security and Culture	Prof Edward Galea
7	Beneficiary	BeSeCu	Germany	Ernst-Moritz-Arndt-Universität Greifswald	Prof. Silke Schmidt
8	Beneficiary	BODE	France	CS Systèmes d'Information	Olivier Balet
9	Beneficiary	CITRINE	France	Thales Security Systems	Christian Fedorczak
10	Beneficiary	COCAE	Greece	Technological Educational Institute of Halkida	Dr. Lambropoulos
11	Beneficiary	COCAE	Germany	FREIBURGER MATERIALFORSCHUNGSZENTRUM	Mr. Klaus-Dieter Dueformantel
12	Beneficiary	COPE	Finland	VTT Technical Research Centre of Finland	Jari Hamalainen
13	Beneficiary	COPE and SICMA	Germany	Centre for European Security Strategies	Reinhard W. Hutter
14	Beneficiary	CrisComScore	Finland	Univ. Jyväskylä Yliopisto	Marita Vos
15	Beneficiary	EFFISEC	France	Sagem Securite	Krassimir Krastev
16	Beneficiary	EUSECON	Germany	German Institute for Economic Research - Department of International Economics	Prof. Dr. Tilman Bruck
17	Beneficiary	FESTOS	Germany	Institute for Cooperation Management and Interdisciplinary Research	Roman Peperhove
18	Beneficiary	FRESP	Belgium	Royal Military Academy	Dr. Peter Lodewyckx
19	Beneficiary	Gate	Greece	Exodus	Anasrasia Garbi
20	Beneficiary	HAMLET	Germany	ESG Elektroniksystem - und Logistik GmbH	Manfred Müller (note: completed in writing only)
21	Beneficiary	iDetecT 4ALL	Belgium	Royal Military Academy Belgium	Peter Lodewyckx
22	Beneficiary	iDetecT 4ALL	UK	Instro Precision Ltd (SME)	John Morcom
23	Beneficiary	iDetecT4All	Belgium	Arttic Brussels	Paul Crompton
24	Beneficiary	IMSK	Sweden	Saab Group	Cecilia Alkhagen
25	Beneficiary	IMSK	UK	Integrated Mobile Security Kit	David Dodsworth
26	Beneficiary	INDECT	Poland	Akademia Gomiczo-Hutnicza im. Stanisława Staszica w Krakowie	Andrzej Dziech
27	Beneficiary	ISCAPS	France	Sagem Securite	Jean-Marc Suchier
28	Beneficiary	ISOTREX	Italy	Enea	Antonio Palucci
29	Beneficiary	MARIUS	France	EADS DSS	Philippe Chrobocinski
30	Beneficiary	OPERAMAR	France	Thales Underwater	Bernard Gamier
31	Beneficiary	PALMA	France	EADS CCR	Gilles Fournier
32	Beneficiary	PATIN	Germany	Diehl BGT Defence, Überlingen	Klaus Scheerer,
33	Beneficiary	SECCONDD	UK	Secure Container Data Service Standardisation	Michael Naylor
34	Beneficiary	SecurEau	France	Université Henri Pointcaré	Sylvain Fass
35	Beneficiary	SecurEau	Finland	KANSANTERVEYSLAITOS	Jaakko Penttinen

List of interviews

A

36	Beneficiary	SECURNEV	Germany	Adelphi Research	Achim Maas
37	Beneficiary	SGL for USaR	Greece	National technological university of Athens	Mr Statheropoulos
38	Beneficiary	SOTERIA	Belgium	Katholieke Universiteit Leuven	Giovanni Lapenta
39	Beneficiary	SUBITO	UK	Selex Gallileo	Dr Mark Daniell David Humphre
40	Beneficiary	TERASEC	UK	Active Terahertz Imaging For Security	David A Ritchie
41	Beneficiary	TERASEC	Germany	Deutsches Zentrum für Luft- und Raumfahrt e. V (German Aerospace Center)	Dr. Heinz-Wilhelm Hübers
42	Beneficiary	UNCOSS	France	Eca SA	Nicolas OUDOT
43	Beneficiary	UNCOSS	Croatia	Ruder Boskovic Institute	Jasmina Obhodas
44	Beneficiary	WIMA ² S	France	Thales Airborne Systems SA	Gilles Jurquet
45	Beneficiary	SecureSME		Name TBC	
46	End –user	NMFRDisaster	DK	Danish Red Cross	Nana Wideman
47	National Authority	N/A	Denmark	EuroCenter Danish Agency for Science, Technology and Innovation	Anette Birch
48	National Authority	N/A	Czech Rep	Academy of Sciences of the Czech Republic	Eva Hillerova
49	National Authority	N/A	Sweden	Swedish Defense Research Agency (FOI)	Hans Frennberg
50	National Authority	N/A	Germany	VDI TECHNOLOGIEZENTRUM GMBH	Karin Wey (Steffen Muhle)
51	National Authority	N/A	Belgium	STIS	Kristof Vlaeminck, replaces Pascale Van Dinter
52	National Authority	N/A	Poland	The Institute of Fundamental Technological Research PAN	Renata Ryerz
53	NCP	N/A	UK	National Contact Point Security Research UK, Office for Security and Counter-Terrorism, the Home Office	Dr Brian Hampson
54	NCP	N/A	GR	Help-Forward - Forth	Vangelis Argoudelis
55	NCP	N/A	IT	APRE	Iacopo de Angelis
56	Selected Representative	N/A	Belgium	ESRIF- EP ITRE Committee	Angelika Niebler
57	Industry	N/A	Sweden	IMG-S	Hakan Enquist
58	Selected Representative	N/A	Sweden	ESRIF	Helena Lindberg (changed to Sundelius Bengt)
59	Wider Stakeholders	N/A	Belgium	FFG	Jeanette Klunkat
60	Wider Stakeholders	N/A	Belgium	EDA	Utimea Madalamo
61	Wider Stakeholders	N/A	EU	EDA	Hilary Davies
62	Industry	N/A	Belgium	IMG-S	Pierre-Alain Fonteyne,
63	Potential beneficiary	N/A	UK	Astrium EADS	Keith Smith
64	NCP	N/A	Austria	FFG – Austrian Research Promotion Agency	Andrea Hoffman
65	NCP	N/A	Netherlands	EG-Liaison	Paul Kruis

List of interviews

A

66	NCP	N/A	Belgium	STIS (Scientific and Technical Information Service)	Pascale van Dinter
67	Selected Representative	N/A	Belgium	ESRIF / European Parliament	Angelika Niebler
68	Selected Representative	N/A	Belgium	European Defence Agency	Utimia Maddaleno
69	End-user(prospective)	N/A	Netherlands	TNO Defensie en Veiligheid	Ruud Busker
70	End-user	Patin	Belgium	Eurocontrol	Rainer KÖLLE
71	Beneficiary and end-user	SecurEau	UK	Veolia Water	Mick O'Malley
72	Beneficiary (and end-user)	EU-SECII	Italy	United Nations Interregional Crime and Justice Research Institute	Alberto Contaretti
73	End-user	CrisComScore	Finland	Emergency Services College Finland (supervised by Ministry of the Interior - College provides vocational training for rescue services and emergency response)	Hannu Rantanen
74	End-user (prospective)	N/A	UK	Police National CBRN Centre	Andy Sigsworth
75	End-user (prospective) and industry	N/A	UK	British Airways (BA)	Andrew Dyer
76	End –user (prospective)	ESRIF	Germany	Federal Office of Civil Protection and Disaster Assistance (BBK)	Christoph Unger (Bette Coellen)
77	End –user (prospective)	N/A	UK	International Institute for Strategic Studies (IISS)	Bastian Giegerich
78	End –user (prospective)	N/A	UK	Former Director Government Communication Head Quarters (GCHQ)	Sir David Omand GCB
79	End-user/Partner	CREATIF	UK	Federal Institute for Materials Research and Testing Division VIII.3: Non-Destructive Testing / Radiological Methods	Jörg Beckmann
80	End-user/Partner	UNCOSS	Croatia	Port Authority Vukovar	Ivan Suker
81	End-user/Partner	Samurai	UK	BAA	Stephen Challis
82	End-user/Partner	UNCOSS	France	COMMISSARIAT ENERGIE ATOMIQUE CEA	Guillaume Sannie
83	End-user/Partner	CITRINE	Poland	ESAProjekt Sp. z o.o.	Rafał Dunał
84	End-user/Partner	WIMAAS	Belgium	EUROSENSE BELFOTOP N.V.	Julie Deleu
85	End-user/Partner	CREATIF	The Netherlands	TNO Defense, Security and Safety Business Unit Biological and Chemical Protection	Maarten S. Nieuwenhuizen
86	End –user (prospective)	N/A	UK	Resilience Industries Suppliers Community (RISC) / UK Aerospace, Defence, and Security (ADS)	Hugo Rosemont
87	End –user (prospective)	N/A	UK	Deputy Director, CBRNE Office of Security and Counter Terrorism in the Home Office (OSCT)	Angela Singh

List of interviews

A

88	End –user (prospective)	N/A	UK	Home Office Office of Security and Counter Terrorism in the Home Office (OSCT) CBRNE team (Explosives)	Tim Dignan
89	End –user (prospective)	N/A	UK	CEO of Selex-Si-Uk, and Chairman, RISC International	Michael Clayforth-Carr
90	End –user (prospective)	N/A	UK	Non Exec Director of Smiths Detection, and member of RISC International	John Backhouse
91	End –user (prospective)	N/A	UK	Industry Secondee to OSCT and UK member of FP7 Security Advisory Group	Adam Ogilvie-Smith
92	End –user (prospective)	N/A	UK	UK Member of FP7 Security Advisory Group	Andrew Sleight
93	NCP	N/A	UK	FP7UK Contact Point for Security	Derek Gallaher
94	End –user (prospective)	N/A	UK	Innovative Science and Technology in Counter-Terrorism programme to support UK counter terrorism strategy	Graham Attrill
95	End –user (prospective)	N/A	UK	Export Services Executive British Security Industry Association	Caroline Strickley
96	End –user (prospective)	N/A	UK	Director of Transnational Threats and Political Risk (IISS), Former Assistant Chief and Director for Operations and Intelligence of Secret Intelligence Service	Nigel Inkster CMG
97	End-user/Partner	EUSECON	ES	Ingenieria de Sistemas para la Defensa de España, S.A	Carlos Martí Sempere
98	End-user/Partner	COCAE	ES	Universidad Autonoma de Madrid Departamento de Fisica de Materiales	Ernesto Diéguez
99	End-user/Partner	SOBCAH	ES	INDRA SISTEMAS S.A	Sonia Gracia Anadón
100	End-user/Partner	NMFR Disaster	ES	SAMUR proteccion Civil Ayuntamiento de Madrid	Ms. Pamola Rey
101	End-user/Partner	SGL for USaR	ES	TEMAI Ingenieros S.L. ES	Luis Francisco Bussion Fernandez
102	End-user/Partner	SGL for USaR	ES	UNIVERSIDAD POLITECNICA DE MADRID	Beatriz Cubeiro
103	End-user/Partner	STRAW	ES	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA	Elsa Prieto Pérez
104	End –user (prospective)	N/A	ES	Spanish operator for the National Train Company – RENFE	Jaime Pereira Ballesteros
105	End –user (prospective)	N/A	DE	Regional authority - South Brandenburg Ex-Head of Division "Security Research and Counterterrorism", Ministry of Interior in Brandenburg/Germany.	Dr Stefan von Senger
106	End –user (prospective)	N/A	DE	Regional authority - South Brandenburg Division "Security Research and Counterterrorism", Ministry of Interior in Brandenburg/Germany.	Dr Haike Wagner

List of interviews

A

107	End –user (prospective)	N/A	IT	Italian Civil protection Agency Dipartimento della Protezione Civile	Pieluigi Soddu
108	End-user	GATE	IT	Co-ordinator Organised and Economic Crime Study Groups National Financial Intelligence Unit, Banca d'Italia	Massimo Nardo
109	Wider stakeholder	N/A	EU	Director, Innovation, CEN-CENELEC, (European Committee for Standardization) Standardisation Mandate in field of security research	John Ketchell

Bibliography

B

PASR
<p><i>Legal basis, Programme documentation, Calls for Proposals and data on programme statistics</i></p> <ul style="list-style-type: none"> • Annual Programme of Work 2004, 2005, 2006 for the Preparatory Action in the field of Security Research • First, second and third Calls for Proposals for the Preparatory Action on "The enhancement of the European industrial potential in the field of Security Research" (2004, 2005, 2006) • Statistics on the outcomes of these calls, budgetary allocations (planned, actual)
FP7 Theme 10 Security
<p><i>Legal basis, programme documentation, Calls for Proposals and data on programme statistics</i></p> <ul style="list-style-type: none"> • COUNCIL DECISION of 19 December 2006 concerning the Specific Programme "Cooperation" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013). • FP7 in Brief: How to get involved in the EU 7th Framework Programme for Research, 2007 • Rules for the submission of proposals, and the related evaluation, selection and award procedures in FP7, Version 3, 21 August 2008 COM(2008)4617 • Framework Programme and Specific Work Programmes supported through Security Theme 10 (2007, 2008, 2009 calls) • Statistics on the outcomes of these calls, budgetary allocations (planned, actual) • Security Research: towards a more secure society and increased industrial competitiveness, 2009 (Brochure of 45 projects listing all projects funded through the first two call of FP7 – Security) • Security Research: Investing into security research for the benefits of European citizens (September 2010) • 5th Progress Report on SME Participation in the 7th R&D Framework, DG Research, 30.04.10
Security Research – key policy documents and Wider documentation
<p><i>Policy communications – Security Research (general)</i></p> <ul style="list-style-type: none"> • Commission Communication "Implementation of Preparatory Action on the Enhancement of the European industrial potential in the field of security research : Towards a programme to advance European security through Research and Technology C(2004) 249 final • Commission Communication, "Towards a programme to advance European security through Research and Technology", COM(2004) 72 final • Commission Communication: Security Research: The Next Steps (COM 2004 590 final) <p><i>Wider documentation</i></p> <ul style="list-style-type: none"> • ESRIF Final Report, providing an overview of recent debates on Security Research, December 2009 • ESRAB Report – Meeting the challenge: The European Security Research Agenda, 2008 • Report of panel of high-level experts on space and security • Study on the Competitiveness of the EU security Industry, 2009, Ecotec/ Technopolis, commissioned by the Security Unit • Bridging efforts - Connecting Civilian Security and Military Capability Development EDA Special Bulletin : Bridging Efforts, 9 February 2010

Bibliography

B

<ul style="list-style-type: none"> Michael Braun et al, 'Tools and Indicators for Community Research Evaluation and Monitoring' Proneos GmbH, July 2009
<p><i>Policy communications – Security Research (thematic)</i></p>
<p>Aviation security</p> <p>Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (Text with EEA relevance) – Inter-institutional declaration</p> <p>Common rules for safeguarding civil aviation - sky marshals must be "specially selected and trained". Proposed in 2005, adopted March 2008</p> <p>Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security – Additional measures were adopted in November 2006 in response to the Transatlantic Airline Plot COM (2005) 429</p> <p>Council Decision 2007/551/CFSP/JHA Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)</p> <p>Regulation (EC) no 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002</p> <p>Directive Of The European Parliament and of the Council on Aviation Security Charges COM(2009) 217</p> <p>COMMISSION REGULATION (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council</p> <p>Commission Communication: on the Use of Security Scanners at EU airports, Brussels, COM(2010) 311/4 Presentations made at the conference held in June 2010 in Berlin on aviation security (DG ENTR organised)</p>
<p>CBRN</p> <p>Programme to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats (14627/2002)</p> <p>EU strategy against proliferation of Weapons of Mass Destruction (15708/2003)</p> <p>EU Solidarity Programme on the consequences of terrorist threats and attacks (revised/widened CBRN Programme) 15480/2004</p> <p>European centre for disease prevention and control (851/2004)</p> <p>The European Union Counter-Terrorism Strategy (14469/4/2005), which incorporates the 2004 EU Solidarity Programme on terrorist threats and attacks</p> <p>Community Civil Protection Mechanism (EC /779/2007)</p> <p>Establishment of an Instrument for Nuclear Safety Cooperation (300/2007)</p> <p>EU CBRN Action Plan (15505/1/2009)</p> <p>UK's national CBRN strategy</p>
<p>Crisis management</p> <p>Community Civil Protection Mechanism (Council decision 2001, updated 2007)</p> <p>The Lisbon Treaty Article 222 Solidarity Clause involving mutual aid in time of crisis</p> <p>'Community approach to the prevention of natural and man-made disasters'</p> <p>"Towards a European Security Model." Outline of the internal mechanisms to be developed to improve</p>

Bibliography

B

internal security in Europe. Based on significant role for community approaches.

"The EU programme for Global Monitoring for Environment and Security (GMES): governance and financing". Presents GMES and emphasizes its strategic importance for the European Union. Through a comparison with the Galileo Programme it also identifies and analyses a set of potential pitfalls. Several political recommendations are presented in the study to help making GMES sustainable and efficient on the long-run.

Land border and maritime security

Regulation (EC) No 724/2004 amending Regulation (EC) No 1406/2002 establishing a European Maritime Safety Agency

Regulation (EC) No 725/2004 on enhancing ship and port facility security

Directive 2005/65/EC on enhancing port security

Commission Regulation (EC) No 324/2008 laying down revised procedures for conducting Commission inspections in the field of maritime security

Preventing Terrorism in Maritime Regions Case Analysis of the Project Poseidon, Edited by Timo Hellenberg and Pekka Visuri, Aleksanteri Papers 2009

Security & Defence Agenda SDA Discussion Paper - The Question Marks over Europe's Maritime Security, Security & Defence Agenda (SDA) Paper November 2007

Presentations made at the conference held in May 2010 on maritime security (DG ENTR organised)

Networked systems and interoperability

Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM (2006)786 final – Official Journal C 126 of 7 June 2007

SMES

4th Progress Report on SME Participation in the 7th R&D Framework, DG Research, 30.09.09

5th Progress Report on SME Participation in the 7th R&D Framework, DG Research, 30.04.10

Eurostat, European business — Facts and figures 2009

Small Business Administration, The Small Business Economy 2009; A Report to the President

Eurostat, Statistics in Focus 71/2009 'SMEs were the main drivers of economic growth between 2004 and 2006' Sept 09

Other

European Drugs Strategy (DG JLS)

European Counter-terrorism Strategy (DG JLS)

Interview checklists

C

In this section, interview checklists are provided that have been used to carry out a structured interview programme. In particular, the following tailored interview checklists were developed for different categories of stakeholders:

- FP7 Theme 10 Security Beneficiaries
- PASR Security Beneficiaries
- End-users in FP7 SEC projects
- Prospective end-users of FP7 SEC research outcomes
- Members of the Security Programme Committee and National Contact Points (NCPs)

Interview checklist: FP7 Theme 10 Security Beneficiaries

This interview checklist is targeted at organisations that have participated in security research projects funded through *FP7 Theme 10 Security (2007-2013)*.

Introduction

1. Please provide a **short overview** of your organisation and its activities in the field of security
2. How did you first find out about **EU funding through FP7 Theme 10 Security**? (examples - FP7 National Contact Point, national / EU website on security research, word of mouth through the security research community, a partner organisation approached you directly?)

Application process

3. How did you find the **application process**? How user-friendly was the guidance for applicants? Was sufficiently clear information provided on the: i) aims and objectives of the Call ii) thematic priorities supported in the annual Security Work Programme iii) types of activities eligible?
4. What was the **duration of the process** from application submission through to evaluation selection? Was this in line with expectations? Overall, how well were **contracting procedures** managed and are there any aspects of the process that could be improved?

Project implementation and monitoring

5. How **effectively has the project been implemented** to date? Has progress been in line with expectations? Have there been any particular difficulties and how have these been overcome?
6. How well has **cooperation between partners** worked so far? Did the project bring together partners that had previously worked together, or are new partners mainly included?
7. To what extent and how have **'end-users'¹ been directly involved** in project design, implementation and follow-up? Have they been engaged in R&D activities (including testing), 'non-R&D' activities (e.g. coordination, technical advice, etc.), training, etc.? Has there been any **indirect involvement of end-users?** (e.g. member of advisory group, external consultant)
8. Were any **SMEs included in the consortia?** If yes, what role have SMEs played and how does the nature (and extent) of their role compare with other partner organisations?
9. What approach has been adopted to the **management and leveraging of intellectual property** and (where relevant) to the protection of **classified information?**

¹ Examples of end-users include members of the emergency services, law enforcement agencies (e.g. police, anti-terrorism bodies, customs and border control), public bodies responsible for public health and safety, policy makers responsible for security policies, the security research community and educational institutions

Interview checklists

C

Funding

10. Was the **funding** received appropriate to the type and nature of research activities supported? Could more have been achieved with additional resources, or the same with less resource? How far did EU project funding **leverage in additional funding support**?
11. If you had not obtained EU financing support through FP7 Security, could funding have been obtained from **alternative national sources**? Would the project have gone ahead in the absence of EU funding support, only partially or not taken place at all?

Project results and outcomes

12. What have been the main **research outputs** from the project to date? For example, has your project led to the development of: i) data ii) products iii) services and iv) technologies and v) enhanced capabilities? How useful are these outputs likely to be for end-users? What outputs might be expected from the remainder of your project's implementation?
13. What **results** have been achieved through the project's implementation in terms of research outcomes? How far have **capabilities and knowledge** in the area of security research been strengthened? Have **new and innovative approaches** been developed?
14. What are the principal areas of **value added** that your project has contributed? Examples include strengthening knowledge about user requirements, improved security practices and procedures enhanced operational knowledge, policy knowledge about future security scenarios?
15. To what extent do you think **research outcomes** from your project are likely to be utilised by public sector end-users? Have any factors limited take-up?
16. What types of **end-users are likely to utilise the research deliverables**? Please provide contact details of organisations that are likely to be end-users of the project's outcomes.
17. To what extent are the project's research outcomes likely to have i) **commercial exploitation** and ii) **'dual usage'** potential?
18. Can any **measurable outcomes** be identified? Examples include: the no. of patents registered, the no. of new products and services, the no. of new technologies developed, the no. of end users making use of project outcomes, etc.?
19. What types of **soft outcomes** can be identified linked to the project's implementation? *Examples include improved networking and coordination between relevant security research actors, improved quality of research and information gathering, and the sharing and dissemination of good practices*

Overall value added, policy impacts and funding leverage

20. FP7 Security Research in 2007-2013 has a number of key aims and objectives. To what extent will your project contribute to the promotion of:
 - Improvements in the security of i) Citizens ii) Infrastructure and Utilities iii) Intelligent Surveillance and Border Security and iv) Restoring Security and Safety in case of Crisis?
 - FP7 Security **cross-cutting missions**: i) Systems integration, interconnectivity and interoperability, ii) Security and society and iii) Security Research coordination and structuring?
 - Strengthened industrial competitiveness through the development of critical mass and prevention of the fragmentation of research efforts
 - Stronger and more effective partnerships between (public) users, industry and the research community

Interview checklists

C

Interview checklist: PASR Beneficiaries

This interview checklist is targeted at organisations having participated in security research projects funded through the *Preparatory Actions on Security Research (PASR) 2004-2006*.

Introduction

1. Please provide an **overview** of your organisation and its activities in the security research field

Application process

2. How did you first find out about **EU funding through FP7 Theme 10 Security**? (examples - FP7 National Contact Point, national / EU website on security research, word of mouth through the security research community, a partner organisation approached you directly?)
3. What was the **duration of the process** from application submission through to evaluation selection? Was this in line with expectations? Overall, how well were **contracting procedures** managed and are there any aspects of the process that could be improved?

Project implementation

4. How **effectively was the project implemented**? Was progress made in line with expectations? Were there been any particular difficulties and how were these overcome?
5. How well has **cooperation between partners** involved in your project worked? Did the project bring together partners that previously worked together, or were new partners involved?
6. To what extent and how were **'end-users'** **directly involved** in project design, implementation and follow-up? Have they been engaged in R&D activities (including testing), 'non-R&D' activities (e.g. coordination, technical advice, etc.), training, etc.? Has there been any **indirect involvement of end-users**? Has there been any **indirect involvement of end-users**? (e.g. member of advisory group, external consultant)
7. Were any **SMEs** included in the project? If yes, what role have SMEs played and how does the extent and nature of their role compare with other partner organisations? Has the inclusion of SMEs brought any particular areas of value added?
8. What approach was adopted to the **management and leveraging of intellectual property** and (where appropriate) to the protection of **classified information**?

Funding

9. Was the **level of funding** appropriate to the type of research activities supported? Could more have been achieved with additional resources, or the same with less resource? Did EU project funding **leverage in additional funding support**? From which actors?
10. If you had not obtained EU financing support through PASR, could funding have been obtained from **alternative national sources**? Would the project have gone ahead in the absence of EU funding support, only partially or not taken place at all?

Project results and outcomes

11. What were the main **research outputs** from the project? For example, did your project lead to the development of new: i) data ii) products iii) services and iv) technologies and v) enhanced capabilities? How useful are these outputs for public sector end-users?

² Examples of end-users include members of the emergency services, law enforcement agencies (e.g. police, anti-terrorism bodies, customs and border control), public bodies responsible for public health and safety, policy makers responsible for security policies, the security research community and educational institutions

Interview checklists

C

12. What **results and impacts** were achieved through the project's implementation? To what extent has the project lead to the production of **high quality research outcomes**?
13. What are the main areas of **value added** of your project? Examples include strengthening knowledge about user requirements, improved security practices and procedures enhanced operational knowledge, policy knowledge about future security scenarios?
14. What has been the extent of **'take-up' of research outcomes by public sector end-users**? What factors have encouraged, or conversely limited take-up?
15. What **types of end-users** are most likely to utilise the research deliverables? Please **provide the contact details** of any end-user organisations that have already made use of, or are likely to draw in future on the project's outcomes.
16. To what extent do the project's research outcomes have i) **commercial exploitation** and ii) **'dual usage'** potential?
17. What **'soft' outcomes** can be identified linked to the project's implementation? Examples include improved networking and coordination between relevant security research actors, the sharing and dissemination of good practices, and the improved quality of research and information gathering?

Overall value added and policy impacts

18. To what extent does the **thematic focus**³ in PASR Calls for Proposals reflect the main security challenges that you believe should be addressed through EU security research?
19. Looking ahead to **planning for FP8**, do you believe any **additional thematic priority areas** should be addressed through EU security research post-2013?
20. How far is the project likely to contribute to the **following EU policy aims**? i) Making a demonstrable contribution to improvements in security ii) Strengthening industrial competitiveness iii) development of relevant knowledge and capabilities, iv) development of new technologies or innovations and v) development of scientific and/or technological excellence

³ The five main areas supported under PASR include: i) Optimising security and the protection of networked systems, ii) Protecting against terrorism (including CBRNE), iii) enhancing crisis management, iv) Achieving interoperability and the integration of systems for information and communication and v) Improving situation awareness

Interview checklists

C

Interim evaluation of the activities carried out by DG Enterprise and Industry under the Seventh Framework Programme for Research, Technological Development and Demonstration 2007-2013

FP7 Theme 10 Security Beneficiaries – Supplementary questions for SMEs

The European Commission is very interested to learn more about the experiences of SMEs in *FP7 Security*. These additional questions support the main interview checklist for FP7 beneficiaries.

Questions relating to the period prior to the project getting underway

1. Was the fact that your organisation is an SME **viewed positively by other partners in the consortium** during the initial partner search and secondly the consortium formulation stage? Please explain.
2. What level of **funding did you apply for?** Was this more than the average funding allocated to other partners involved in the project consortium? If yes, what were the reasons for this?
3. What impact did the availability of **higher co-financing rates for SMEs** in FP7 (70%) compared with other kinds of beneficiaries have in increasing the attractiveness of participating in FP7 Security?
4. If you have previously participated in FP6 or its predecessors, how does FP7 Security compare in terms of **rules, procedures and administrative requirements** for SME applicants?
5. How do you believe your **cost base (staff costs, general operating costs, R&D costs)** for participating in FP7 Security Research project differs from those of other beneficiaries such as universities and research institutions, and larger companies? What are the reasons for this?
6. What were the **main benefits** you expected to get out of participation in FP7 Security?

Questions relating to project implementation

7. Please describe the **nature of your role** in the project consortium. How have SMEs been involved in **project delivery?** In specific work packages (WPs) or in all WPs? In R&D and innovation-oriented WPs?
8. To what extent did the fact that SMEs are participating in the project **impact on structuring** the following: i) the consortium overall at the bid stage ii) project implementation including the allocation of tasks and responsibilities in relation to individual WPs?
9. How well has **cooperation worked so far between SMEs and other partners?**
10. To what extent have SMEs contributed to the development of **'state of the art'** in the particular area of security in which you specialise? How far has the involvement of SMEs contributed to **successful innovation?** How does the role of SMEs differ from other consortium participants in this regard?
11. In the case of projects where **intellectual property has been generated**, to what extent have SMEs been involved in i) the *generation* and ii) the *exploitation* of IP. How well do IP sharing arrangements work?
12. Overall, what **value added** do you believe SMEs bring to project consortia?

Interview checklists

C

Interview checklist: PASR and FP7 Security End-Users

*This interview checklist is targeted at **users** that have been involved either in a PASR or an FP7 EU Security Research project funded by the European Commission's DG Enterprise and Industry. End-users may be involved both directly and indirectly in projects. The Commission attaches great importance to ensuring that FP7 Security Research addresses the needs and expectations of end-users from the programme, given their important role as drivers of demand for EU security products and services.*

Users in the context of EU Security Research are defined as organisations that have a role in promoting the security of European citizens. Examples include: law enforcement agencies (e.g. police, anti-terrorism bodies, customs and border control agencies), the emergency services, public agencies and national and regional authorities responsible for public health and safety and security, and the security research community (including academic and research institutes).

End-Users

1. Please provide a **short overview** of your organisation, including its size and main activities (*including the type of organisation: civil protection, police force, emergency service..., and its size*).
2. What are the most important **security challenges** your organisation faces and how closely aligned are these with the priorities being addressed through the project research?)
3. Is your organisation formally part of a **consortium** receiving FP7 funding?
4. To what extent was your organisation **directly involved** in **PASR or FP7 Security research projects?** (*Examples include: helping to design the project, defining user-requirements based on your organisation's needs, serving on a project advisory panel, testing and technology demonstration, other activities such as coordination, training and the provision of technical advice*)
5. Has your organisation been **indirectly involved** in **PASR or FP7 research projects** (*Examples include: serving on external advisory group of end-users, testing products and services developed, participating in a conference or event, taking part in scenario modelling exercises*)
6. Have you **used any project outputs or research outcomes from PASR or FP7 Security?** If yes, what type of FP7 Project outcomes has your organisation used? Would you consider **exploiting research outcomes** beyond the lifetime of the current research project?
7. Can you identify particular technologies or deliverables from EU security research projects that **would not have been developed without European support** e.g. data, services, products, technologies, practices/ procedures, technical standards?
8. What **technologies** will potentially be needed by your organisation to meet the security challenges of the future?
9. What types of technical standards and technologies would help to **foster inter-operability** and **improve the effectiveness of your organisation's work** when cooperating with other public agencies cross-border?
10. Overall, **how useful** do you perceive the Security Research project to have been in addressing the needs of your organisation as an end-user?
11. Do you have any suggestions with regard to i) **strengthening end-user involvement** in EU Security Research in FP7 and ii) **making research outcomes more useful** to end-users? In particular:

Interview checklists

C

- a. How can the **involvement of end-users be strengthened** in i) the planning and definition phase and ii) the implementation of FP7 Security projects iii) dissemination phase?
- b. What could be done to **maximise the potential value added** of project research outcomes from EU Security Research for end-users?
- c. Could anything be done to promote **greater take-up** by end-users of research outcomes?
- d. What are the most effective communication mechanisms for **disseminating information about project research results** to prospective end-users?

Interview checklist: Prospective End-Users of EU Security Research funded through FP7

*This interview checklist is targeted at **potential end-users** of EU Security Research outcomes resulting from projects funded through the 7th Framework Programme for Research and Technological Development.*

Prospective Users of research outcomes

1. What do you view as the main **security challenges** in the area of security for which your organisation is responsible?
2. What types of products, services, technologies, knowledge and capabilities would be most helpful in **meeting the security challenges** you identified in (1)?
3. To what extent do you think that the **types of activities** being supported through FP7 are likely to **meet your needs** as a prospective end-user of research outcomes? (*prior to and during the discussion, we can provide examples of which projects have been supported under particular themes e.g. crisis management, critical infrastructure protection, CBRNE, aviation security, maritime security*)
4. What types of technical standards and new technologies would help to foster **inter-operability and improve the effectiveness of your organisation's work** when cooperating with other public agencies cross-border?
5. What types of research will be needed by your organisation to **meet the European security challenges of the future**? In respect of each of the points below, what **timeframe** will you need these research outcomes in (recognising that there are very long R&D lead-times in some areas)?
6. Do you have suggestions with regard to i) **strengthening user involvement** in EU Security Research in FP7 and ii) **making research outcomes more useful** to end-users? In particular:
 - a. How can the **involvement of end-users be strengthened** in i) the planning and definition phase and ii) the implementation of FP7 Security projects and iii) dissemination phase?
 - b. What could be done to **maximise the potential value added** of project outcomes from EU Security Research for end-users?
 - c. Could anything be done to promote **greater take-up** by end-users of research outcomes?
 - d. What are the most effective communication mechanisms for **disseminating information about project research results** to prospective end-users?

Interview checklists

C

Interview checklist: National Contact Points for FP7 Security

This interview checklist is targeted at National Contact Points for *FP7 Theme 10 Security (2007-2013)* funded by the European Commission.

1. Please provide a short overview of your organisation and its activities in your capacity as the National Contact Point for FP7 Security (and/ or FP Space) research.
2. What level of input (financial and human resources) has your organisation made to promote participation in EU Space and Security research? How does this compare with other areas of FP7?
3. On average, what proportion of time per month does your organisation spend on FP7 space and security related activities? And dealing with enquiries from applicants and potential beneficiaries in these areas?
4. What are the main areas of activity that you undertake in your capacity as an NCP in relation to space and security research? Awareness-raising? Information dissemination? Providing advice and guidance to prospective applicants?
5. What level of interest has there been among the different actors eligible to participate in EU funded space research through FP7 space and security? Do you keep records in respect of the no. of queries that you receive from potential FP7 applicants that contact you in respect of FP7 Space and Security research?
6. What types of queries have you received in relation to FP7 Space and Security research?
7. What proportion of enquiries focused on the provision of advice and guidance to applicants on: i) forthcoming Calls for Proposals ii) current Calls for Proposals and Guidance for Applicants once a given Call has been launched iii) follow-up to Calls, such as queries from unsuccessful applicants?
8. To what extent does the level of interest from potential applicants differ between activity area and type of FP7 funding scheme (e.g. Collaborative Project, Coordination and Support Action)?
9. What in your view are satisfaction levels among applicants in respect of FP7 Space and Security research with regard to i) the clarity and user-friendliness of information in Calls for Proposals ii) the amount and quality of information dissemination and iii) the quality of advisory and support provided by NCPs?
10. What have been the main strengths so far in relation to the management and implementation of FP7 Space and Security? Are there any weaknesses that should be highlighted? To what extent (and how, if at all) could the programme have been managed more effectively?
11. How well has cooperation and information sharing worked between the Commission, the REA and the NCPs?
12. How far has FP7 Space and Security research succeeded in attracting applicants and participants from leading-edge, world-class research organisations? How does this vary between space and security?
13. Has your organisation been involved in the SEREN* or COSMOS* projects? If yes, how effective has this been in improving the quality of service provision, networking and coordination on FP7 Space and Security?

Interview checklists

C

Interview checklist: Members of the FP7 Security Programme Committee and National Authorities

This interview checklist is targeted at National Authorities and members of the Security Programme Committee in *FP7 Theme 10 Security (2007-2013)* funded by the European Commission.

1. Please provide a short overview of your organisation and its activities as these relate to space and security research.
2. Please provide an overview of the national security policy and institutional framework in your Member State and identify the main funding programmes / schemes (if any)
3. What are the main challenges and threats in respect of security policy at national, European and international level? To what extent are these challenges being addressed through FP7 SEC?
4. Are there any areas of overlap between EU space research and national activities being supported in the 2007-13 period (European Added Value)? In what ways, if any, does EU Security research complement national publicly financed interventions in this area? Are there any differences in respect of the types of interventions being supported?
5. What are your experiences of participating in the FP7 Security Programme Committee? To what extent has the Committee been effective in respect of each of the following:
 - i) Reviewing the Commission's list of ranked proposed projects following each Call for Proposals?
 - ii) Finalising the selection of projects to be funded
 - iii) Ensuring that the ethical dimension has been fully taken into account in the project selection process
 - iv) Ensuring a good balance in the types of projects being funded
6. Is there an appropriate mix in your view between the different types of projects supported, for example, projects leading to the development of new technologies, focusing on the development of security hardware, research projects to strengthen knowledge and understanding about different aspects of EU Security Research?
7. In your view, what have been the main strengths so far in relation to the management and implementation of FP7 Space and Security? Do you have any comments with regard to the role and effectiveness of the Commission and the REA respectively in this regard?
8. Are there any weaknesses that should be highlighted? To what extent (and how, if at all) could the programme have been managed more effectively?
9. Are you satisfied that the PASR Preparatory Action in the area of Security and FP7 Security Research have succeeded in attracting the EU's best researchers, research organisations and leading companies?
10. Looking ahead, are there any new or additional areas of research that should be funded through EU Security Research in the remainder of FP7 or in FP8?

Interview checklists

C

Interim evaluation of the activities carried out by DG Enterprise and Industry under the Seventh Framework Programme for Research, Technological Development and Demonstration 2007-2013

FP7 Theme 10 Security Beneficiaries – Supplementary questions for SMEs

The European Commission is very interested to learn more about the experiences of SMEs in *FP7 Security*. These additional questions support the main interview checklist for FP7 beneficiaries.

Questions relating to the period prior to the project getting underway

1. Was the fact that your organisation is an SME **viewed positively by other partners in the consortium** during the initial partner search and secondly the consortium formulation stage? Please explain.
2. What level of **funding did you apply for?** Was this more than the average funding allocated to other partners involved in the project consortium? If yes, what were the reasons for this?
3. What impact did the availability of **higher co-financing rates for SMEs** in FP7 (70%) compared with other kinds of beneficiaries have in increasing the attractiveness of participating in FP7 Security?
4. If you have previously participated in FP6 or its predecessors, how does FP7 Security compare in terms of **rules, procedures and administrative requirements** for SME applicants?
5. How do you believe your **cost base (staff costs, general operating costs, R&D costs)** for participating in FP7 Security Research project differs from those of other beneficiaries such as universities and research institutions, and larger companies? What are the reasons for this?
6. What were the **main benefits** you expected to get out of participation in FP7 Security?

Examples include: networking and relationship building with international partners, developing stronger relationships with large companies, access to research centres of excellence, the development of research and innovation and technical knowledge, the opportunity to generate and exploit IP, strengthening knowledge about end-user requirements for security research, participation in future EU FP programmes, developing new consultancy and other opportunities to exploit knowledge and expertise, etc.

Questions relating to project implementation

7. Please describe the **nature of your role** in the project consortium. How have SMEs been involved in **project delivery?** In specific work packages (WPs) or in all WPs? In R&D and innovation-oriented WPs?
8. To what extent did the fact that SMEs are participating in the project **impact on structuring** the following: i) the consortium overall at the bid stage ii) project implementation including the allocation of tasks and responsibilities in relation to individual WPs?
9. How well has **cooperation worked so far between SMEs and other partners?**
10. To what extent have SMEs contributed to the development of **'state of the art'** in the particular area of security in which you specialise? How far has the involvement of SMEs contributed to **successful innovation?** How does the role of SMEs differ from other consortium participants in this regard?
11. In the case of projects where **intellectual property has been generated**, to what extent have SMEs been involved in i) the *generation* and ii) the *exploitation* of IP. How well do IP sharing arrangements work?
12. Overall, what **value added** do you believe SMEs bring to project consortia?

Selection of Security Research projects

D

Project Selection

Having conducted a review of PASR and FP7 Security projects included in the May 2009 project compendium, and of the complete list of PASR projects provided by DG ENTR, we have made a provisional selection of projects for the thematic case studies. It should be noted that at this stage we have not selected projects for examination in respect of the horizontal case study on SMEs – this will be determined once a more thorough assessment of project partners has been undertaken (it is often difficult to know until the research is underway and lead partners have been contacted the extent to which SMEs have been involved in particular projects):

Selection of FP7 projects

NO.	ACRONYM	PROJECT TITLE	BUDGET	CASE STUDY THEMES	LEAD PARTNER (COUNTRY)
1	AMASS	Autonomous Maritime Surveillance System	€ 3,580,550	Maritime surveillance	DE
2	OPERAMAR	An InterOPERable Approach to European Union MARitime Security Management	€ 669,132	Maritime surveillance	FR
3	SECTRONIC	Security System for Maritime Infrastructure, Ports and Coastal Zones	€ 4,496,414	Maritime surveillance	UK
4	UNCOSS	UNDERWATER COASTAL SEA SURVEYOR	€ 2,780,000	Maritime surveillance	FR
5	WIMA ² S	WIDE MARITIME AREA AIRBORNE SURVEILLANCE	€ 2,737,169	Maritime surveillance	FR
6	EFFISEC	Efficient Integrated Security Checkpoints	€ 10,034,837	Maritime surveillance and aviation security	FR
7	iDeteCT 4ALL	Novel Intruder Detection and Authentication Optical Sensing Technology	€ 2,298,014	Aviation security	UK
8	SAMURAI	Suspicious and Abnormal behaviour Monitoring Using a network of cameras & sensors for situation awareness enhancement	€ 2,478,052	Aviation security	UK
9	SUBITO	Surveillance of Unattended Baggage and the Identification and Tracking of the Owner	€ 2,581,055	Aviation security	UK
10	CREATIF	Related testing and certification facilities	€ 831,300	CBRNE	AU
11	IMSK	Integrated Mobile Security Kit	€ 14,864,308	CBRNE	SE
12	LOTUS	Localization of Threat Substances in Urban Society	€ 3,189,146	CBRNE	SE
13	OPTIX	Optical Technologies for	€ 2,487,556	CBRNE	ES

Selection of Security Research projects

D

		Identification of Explosives			
14	SecurEau	Security and decontamination of drinking water distribution systems following deliberate contamination	€ 5,269,168	CBRNE	FR
15	FRESP	Advanced First Response Respiratory Protection	€ 3,029,967	CBRNE and crisis management	BE
16	COCAE	COOPERATION ACROSS EUROPE FOR Cd(Zn)Te BASED SECURITY	€ 2,037,610	CBRNE (plus aviation security and maritime surveillance)	GR
17	BeSeCu	Human behaviour in crisis situations : A cross cultural investigation in order to tailor security-related communication	€ 2,093,808	Crisis management	DE
18	COPE	COMMON OPERATIONAL PICTURE EXPLOITATION	€ 2,535,049	Crisis management	FI
19	NMFRDisaster	Identifying the Needs of Medical First Responders in Disasters	€ 815,079	Crisis management	IS
20	FORESEC	Europe's evolving security: drivers, trends and scenarios	€ 942,202	Crisis management	FI
21	SECRICOM	Seamless Communication for Crisis	€ 8,606,791	Crisis management	UK
22	SGL for USaR	Second Generation Locator for Urban Search and Rescue Operations	€ 4,859,026	Crisis management	GR
23	SICMA	Simulation of Crisis Management Activities	€ 2,566,330	Crisis management	IT
24	CRESCENDO	Coordination action on risks, evolution of threats and context assessment by an enlarged network for an R&D roadmap	€ 499,523	N/A	FR
25	CrisComScore	Developing a crisis communication scorecard	€ 1,013,207	N/A	FI
26	ADABTS	Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces	€ 4,478,990	N/A	SE
27	ESCORTS	European network for the security of control and real-time systems	€ 1,076,091	N/A	BE
28	EU-SECII	Coordinating National Research Programmes and Policies on Security at Major Events in Europe	€ 2,527,000	N/A	IT
29	EUSECON	A new agenda for European Security Economics	€ 3,000,736	N/A	DE
30	FESTOS	Foresight of Evolving Security Threats Posed by Emerging Technologies	€ 1,232,976	N/A	IL

Selection of Security Research projects

D

31	INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment	€ 14,863,988	N/A	PL
32	Secumev	Assessment of environmental accidents from a security perspective	€ 851,245	N/A	HU

53 grant agreements had been signed as at 01.01.2010 following the first two SEC calls for proposals in FP7. Of these, we proposed examining 23 of the 53 for the purposes of the case studies.

Selection of PASR projects

NO.	ACRONYM	PROJECT TITLE	PASR CALL	BUDGET	CASE STUDY THEMES	LEAD PARTNER (COUNTRY)
1	ISCAPS	Integrated surveillance areas for public security	2004	€ 1,699,999	Aviation security	FR
2	TERASEC	Protection of air transportation and infrastructure from terrorism	2004	€ 2,149,679	Aviation security	DE
3	PALMA	Protection of airliners against manpads attacks	2005	€ 1,457,000	Aviation security/ CBRNE	FR
4	PATIN	Protection of air transportation and infrastructure from terrorism	2005	€ 2,651,542	Aviation security/ CBRNE	DE
5	ISOTREX	Integrated system for on-line trace explosives detection in solid and vapour state	2006	€ 1,242,265	CBRNE/ aviation security	IT
6	IMPACT	Innovative measures for protection against terrorism	2004	€ 2,717,640	CBRNE	NL
7	TIARA	Treatment initiatives after radiological accidents	2004	€ 171,900	CBRNE	FR
8	AEROBACTICS	Assessment of the quality, identity, viability, origin and dispersion of airborne micro-organism for application in crisis management tools	2006	€ 951,923	CBRNE/crisis management	DK
9	BODE	Biological Optical Detection Experiment	2006	€ 1,815,614	CBRNE	FR
10	HAMLET	Hazardous Material localisation and Person tracking	2006	€ 218,823	CBRNE	DE
11	WATERSAFE	On-line monitoring of drinking water for public security from deliberate or accidental contamination	2006	€ 1,923,976	CBRNE, SMEs	UK
12	CRIMSON	Urban crisis simulation systems	2004	€ 1,520,000	Crisis management	FR
13	ASTRO+	Advanced space technologies support security operations	2004	€ 2,200,000	Crisis management	FR
14	GEOCREW	Study on geo-data and crisis early warning situation awareness	2004	€ 399,851	Crisis management	DE

132

Selection of Security Research projects

D

15	MARIUS	Monitoring crisis management operation	2005	€ 1,425,402	Crisis management	FR
16	PROBANT	Crisis management people	2005	€ 1,176,799	Crisis management	FR
17	CITRINE	Common Intelligence and Traceability for Rescue and Identification Operations	2006	€ 1,412,606	Crisis management	FR
18	SOBCAH	Surveillance of borders coastlines	2005	€ 2,010,600	Maritime surveillance	IT
19	SECCONDD	Secure Container Data Service Standardisation	2005	€ 399,851	Maritime surveillance	UK
20	SECURESME	Supporting Security Field SMEs preparing RTD projects	2006	€ 256,928	SMEs	PT
21	BIO3R	Bioterrorism resilience, research, reaction	2006	€ 642,067	CBRNE	FR
22	CITRINE	Common intelligence and transparency for rescue and identification operations	2006	€ 1,883,475	N/A	FR
23	GATE	Next generation anti-terrorism financing (ATF) Methods	2006	€ 1,133,078	N/A	GR
24	STACCATO	Stakeholders platform for supply chain mapping, market conditions analysis and technologies opportunities	2006	€ 695,141	N/A	BE
25	STARBORSEC	Standards for Border Security Enhancement	2006	€ 680,837	N/A	FR

In respect of the PASR Preparatory Action funded in FP6, 39 projects were supported across 3 annual Calls for Proposals (2004, 2005 and 2006 respectively). Each Call had a budget of 15m euros. We have selected 20 of the 39 projects for the purposes of the thematic case studies.

In the case of each project, we have interviewed:

- The **lead coordinator**
- A minimum of **one additional partner** in the consortium (either face to face or by phone as was deemed appropriate)
- Where possible, one or two **users**, where these have been directly included in the consortium

Additional projects were also examined as part of the wider research on topics such as networking to strengthen the competitiveness and promote greater cooperation between key actors in the security industry, projects focusing on inter-operability, mass transit systems and those that promote the development of standards and harmonisation. There are two projects with a strong SMEs component (one focusing on encouraging the participation of SMEs in EU funded security research, the other having strong participation of SMEs).

Indicators paper

E

A working paper on indicators is provided as a separate attachment. This provides a more detailed assessment of the main issues in relation to the development of a detailed monitoring framework on monitoring and indicators. Key issues on indicators are summarised in the main evaluation report (Section 3.2).

Full survey results

F

Security Beneficiaries Survey Response Tables

Organisation	No	%
Large company (250 and over employees)	20	27.8
Subsidiary of large company	3	4.2
SME (under 250 employees)	14	19.4
Research institute	14	19.4
University	12	16.7
Public body/company (first responder, police, civil protection, ambulance or health services)	2	2.8
Public authority (national, regional)	3	4.2
Other	4	5.6
Total	72	100.0

Employees	No	%
0-9 employees	6	8.3
10-49 employees	12	16.7
50-249 employees	11	15.3
Over 250 employees	43	59.7
Total	72	100.0

Country	No	%	Country	No	%
Albania	0	0.0	Liechtenstein	0	0.0
Austria	1	1.4	Lithuania	0	0.0
Belgium	3	4.2	Luxembourg	0	0.0
Bosnia and Herzegovina	0	0.0	Macedonia (FYR)	0	0.0
Bulgaria	0	0.0	Malta	0	0.0
Croatia	3	4.2	Montenegro	0	0.0
Cyprus	0	0.0	Netherlands	1	1.4
Czech Rep	0	0.0	Norway	0	0.0
Denmark	2	2.8	Poland	0	0.0
Estonia	0	0.0	Portugal	4	5.6
Faroe Islands	0	0.0	Romania	1	1.4
Finland	3	4.2	Serbia	0	0.0
France	7	9.7	Slovakia	1	1.4
Germany	7	9.7	Slovenia	0	0.0
Greece	3	4.2	Spain	10	13.9
Hungary	1	1.4	Sweden	5	6.9

Full survey results

F

Iceland	0	0.0	Switzerland	0	0.0
Ireland	0	0.0	Turkey	0	0.0
Israel	0	0.0	Ukraine	2	2.8
Italy	12	16.7	UK	6	8.3
Latvia	0	0.0	Total	72	100.0

1.5: Which PASR and FP7 Security project were you mainly involved in?

PASR	Nº	PASR	Nº	PASR	Nº
ADABTS	0	EUSECON	0	RAPTOR	0
AMASS	2	FASTID	0	SAFE-COMMS	0
ARGUS 3D	0	FESTOS	0	SAMURAI	2
BeSeCu	1	FORESEC	1	SCIIMS	0
CAST	0	FRESP	2	SECRICOM	3
COCAE	2	GLOBE	2	SECTRONIC	1
COPE	3	iDeteCt 4ALL	1	SecurEau	1
CPSI	0	IMCOSEC	0	SECURECHAINS	2
CREATIF	1	IMSK	3	SECURENV	1
CRESCENDO	2	INDECT	0	SEREN	0
CrisComScore	0	INDIGO	1	SERON	0
CRISIS	0	INEX	0	SGL for USaR	1
DECOTESSC1	0	INFRA	0	SICMA	0
DEMASST	0	ISTIMES	0	SRC 08	0
DETECTER	0	LOGSEC	0	SRC-09	0
DITSEF	1	LOTUS	1	STAR-TRANS	0
EFFISEC	2	MULTIBIDOSE	0	STRAW	0
EMILI	0	NI2S3	0	SUBITO	0
ESCoRTS	1	NMFRDisaster	0	TALOS	1
ESS	0	Odyssey	0	TASS	0
EULER	1	OPERAMAR	1	UNCOSS	4
EURACOM	0	OPTIX	2	VIRTUOSO	0
EU-SEC II	0	OSMOSIS	0	WIMA²S	1
				Total	47
FP7	Nº	FP7	Nº	FP7	Nº
AEROBACTICS	2	HITS-ISAC	0	SecureSME	5
ASTRO+	4	IMPACT	5	SeNTRE	0
BIO3R	1	ISCAPS	3	SOBCAH	2

Full survey results

F

BIOTesting EUROPE	0	ISOTREX	2	STABORSEC	0
BODE	1	I-TRACS	0	STACCATO	0
BS-UAV	0	MARIUS	1	SUPHICE	0
CITRINE	2	PALMA	3	TERASEC	1
CRIMSON	2	PATIN	1	TIARA	0
ESSTRT	1	PETRA.NET	0	TRIPS	0
EUROCOP	0	PRISE	0	USE IT	0
GATE	0	PROBANT	0	VITA	1
GEOCREW	0	ROBIN	0	Watersafe	0
HAMLéT	0	SECCONDD	1	WINTSEC	3
				Total	41

1.6: Were you the lead co-ordinator or a partner organisation for the project?

Options	No	%
Lead co-ordinator	14	19.4
Partner organisation	58	80.6
Total	72	100.0

1.7: Please describe your role in the project consortium (please tick all that apply)

Options	No	%
R&D	55	76.4
Consultancy / advisory role	14	19.4
Development of knowledge	22	30.6
Dissemination activities	24	33.3
Other	12	16.7

2.1: To what extent do you believe that the objectives of EU Security Research in FP7 are appropriate to the needs of the security research community?

Options	No	%
Highly appropriate	36	50.0
Quite appropriate	33	45.8
Not appropriate – there needs to be a review of the programme's objectives	1	1.4
No response	2	2.8
Total	72	100.0

Full survey results

F

2.2: In applying for PASR and / or FP7 Security Research funding, did you make contact with the National Contact Point (NCP)?

Options	No	%
Yes	27	37.5
No	43	59.7
No response	2	2.8
Total	72	100.0

If you did make contact with your NCP, how useful was the information, advice and guidance provided:

Options	No	%
Very useful	12	44.4
Somewhat useful	12	44.4
Not very useful	3	11.1
Not useful at all	0	0.0
No response	0	0.0
Total	27	100.0

2.3: With regard to the consortium's partnership structure, does the project mainly involve partners that previously cooperated with one another, new partners, or a combination?

Options	No	%
Partners that previously cooperated	4	5.6
A combination of new partners and those with whom we have previously worked	54	75.0
Entirely new partners brought together specifically to participate in EU funded security research	12	16.7
No response	2	2.8
Total	72	100.0

3.1: How well have contracting procedures been managed by the Commission?

Options	No	%
Very well	21	29.2
Quite well	40	55.6
Not well	8	11.1
Not at all well	1	1.4
No response	2	2.8
Total	72	100.0

Full survey results

F

3.2: How well has project monitoring been carried out?

Options	No	%
Very well	20	27.8
Quite well	44	61.1
Not well	5	6.9
Not at all well	0	0.0
No response	3	4.2
Total	72	100.0

3.4: Was the funding allocation sufficient to achieve your project's objectives?

Options	No	%
Yes, the funding was satisfactory	29	40.3
Yes, but we could have achieved better research outcomes with a larger budget	38	52.8
No, the funding is insufficient to achieve project objectives	2	2.8
No response	3	4.2
Total	72	100.0

3.5: If your project had not received funding through FP7, do you think that you would have been able to secure funding from an alternative source at national or European level?

Options	No	%
Yes	2	2.8
No	47	65.3
Don't know	19	26.4
No response	4	5.6
Total	72	100.0

3.6: If you had not received FP7 funding, would your project still have gone ahead on the same basis?

Options	No	%
Yes, the project would have gone ahead in full	1	1.4
Yes, but only partially	15	20.8
No, the project could not have gone ahead	53	73.6
No response	3	4.2
Total	72	100.0

Full survey results

F

4.1: What sorts of activities have taken place through the project to date? (please tick all that apply)

Options	No	%
R&D activities	49	68.1
Security systems integration	32	44.4
Inter-operability	26	36.1
Field demonstration(s)	31	43.1
Networking activities and information exchange	42	58.3
Dissemination and/or awareness-raising activities (including good practice exchange)	35	48.6
The organisation of workshops meetings, conferences, events	47	65.3
Activities relating to end-user engagement	41	56.9
Exchanges of personnel	4	5.6
Activities relating to the ERA-NET action	0	0.0
The creation of databases	15	20.8
Research leading to the production of papers or publications on security research	36	50.0
Research to identify security trends and future scenarios	35	48.6

4.2: How effective has the role been played by the lead coordinator in managing the following:

Options	Project management aspects		Monitoring and reporting processes to the Commission/ REA		The coordination of research activities	
	No	%	No	%	No	%
Very effective	29	40.3	25	34.7	18	25.0
Quite effective	23	31.9	28	38.9	24	33.3
Not very effective	7	9.7	7	9.7	13	18.1
Not effective at all	1	1.4	0	0.0	2	2.8
No response	12	16.7	12	16.7	15	20.8
Total	72	100.0	72	100.0	72	100.0

4.3: How well has cooperation between partners in the project consortium worked to date?

Options	No	%
Very well	19	26.4
Quite well	48	66.7
Not well	2	2.8
Not at all well	0	0.0

Full survey results

F

No response	3	4.2
Total	72	100.0

4.4(a): Were end-users directly included in the project consortium?

Options	No	%
Yes	50	69.4
No	18	25.0
No response	4	5.6
Total	72	100.0

4.4(b): If yes, were end-users directly involved in project activities?

Options	No	%
Yes, they have been significantly involved in the project consortium and in project activities	25	50.0
Yes, but their involvement has been limited	20	40.0
No	5	10.0
Total	50	100.0

4.5(a): Was a formal advisory panel of end-users set up?

Options	No	%
Yes	28	38.9
No	37	51.4
No response	7	9.7
Total	72	100.0

4.5(b): If yes, what role has the advisory panel played during the project's implementation?

Options	No	%
Major role	9	32.1
Minor role	18	64.3
Minimal role	1	3.6
Total	28	100.0

4.6: Which aspects of project implementation have end-users been involved in to date? (please tick all that apply)

Options	No	%
Member of (internal) advisory group of end-users	23	31.9

Full survey results

F

The project design process	18	25.0
Contributing to operational knowledge or procedures	43	59.7
The testing phase	30	41.7
The definition of future scenarios	36	50.0

4.7: Have users also been indirectly involved in the project?

Options	No	%
Yes	49	68.1
No	15	20.8
No response	8	11.1
Total	72	100.0

4.8: If you responded yes, how have end-users been involved? (please tick all that apply)

Options	No	%
Member of (external) advisory group of end-users	16	32.7
External consultant to project	11	22.4
Testing of data, products and services	11	22.4
Testing of new technologies	12	24.5
Participation in workshops (to identify end user-needs, define future scenarios, etc.)	36	73.5

5.1(a): The European Commission is in the process of developing an indicator system to assess the effectiveness of projects financed through FP7 Security. Which of the following possible indicators do you think could be useful to judge the success of security research projects?

Options	No	%
New data developed	33	45.8
New products developed	43	59.7
New services developed	32	44.4
New technologies developed	50	69.4
New patents developed	22	30.6
New patents registered	16	22.2
Other forms of Intellectual Property developed	16	22.2
End-users making use of project outcomes	50	69.4
Technology efficiency improvements	34	47.2
Creation of knowledge	42	58.3
Creation of new standards and promotion of harmonisation	36	50.0
Enhancement of capabilities in particular areas of civil security	38	52.8

Full survey results

F

(please tick all that apply)

5.1 (b) Where possible, please provide data for any research results that can be quantified:

Options	No
No. of patents developed	6
No. of patents registered	3
No of other forms of Intellectual Property developed	14
No. of data sources	60
No of products developed	33
No. of new services developed	10
No. of new technologies developed	40
No. of knowledge tools (e.g. databases)	16
No. of good practice tools	15
No. of research papers	154
No. of citations	141
No. of end-users (organisations making use of research project outcomes)	21

5.3: What other types of research outcomes (non-quantifiable, soft) can be identified linked to your project to date? (please tick all that apply)

Options	No	%
Progress towards 'state of the art' (note: the highest level of development of a device, procedure, process, technique, technology or area of research reached at any particular time)	43	59.7
Fostering of research excellence	23	31.9
Improved networking and coordination between security research actors	39	54.2
Improved information and good practice sharing between security research actors	26	36.1
Strengthened cooperation between SMEs and large firms	28	38.9
Strengthened innovation transfer between industry and publicly funded research	18	25.0
Increased visibility of new and emerging areas of security research (e.g. the economics of security, the environmental aspects of security etc.)	21	29.2
Greater ability to predict future challenges, threats and developments in different areas of security field	26	36.1
Promotion of standards, harmonisation and interoperability	15	20.8
Other	3	4.2

5.4: What types of end-users are likely to benefit from the results produced through your project? (please tick all that apply)

Full survey results

F

Options	No	%
Regional or local authorities	31	43.1
National authorities	51	70.8
Universities or Higher Education Institutions	10	13.9
Public research institutions	18	25.0
Small and Medium Sized Enterprises (SMEs)	20	27.8
Industry (other than SMEs)	27	37.5
Public agencies responsible for civil security	49	68.1

If you ticked public agencies, please specify what type (*please tick all that apply*):

Options	No	%
Law enforcement agency	23	46.9
Intelligence services	13	26.5
Crisis management and emergency response	33	67.3
Maritime and aviation security agencies	21	42.9
Agencies responsible for chemical, biological, radiological and nuclear safety/ detection	23	46.9
Agencies responsible for public safety and civil security	39	79.6

5.5 To what extent are end-users likely to use the research outcomes produced through your project?

Options	No	%
Highly likely	18	25.0
Somewhat likely	33	45.8
Not likely at all	3	4.2
Difficult to say at this stage in project implementation	6	8.3
No response	12	16.7
Total	72	100.0

5.6: Can you identify any barriers to the uptake of research results developed through your project from an end-user perspective?

Options	No	%
Yes	47	65.3
No	13	18.1
No response	12	16.7
Total	72	100.0

If yes, please tick all that apply:

Full survey results

F

Options	No	%
The results of the research will be useful to end-users, but only after further development	35	74.5
End-users would consider using the results but only if these can be exploited free-of-charge	13	27.7
There may be difficulties in negotiating licensing agreements	6	12.8
There would be prohibitive costs in using the research results (for example, implementing a cross-border IT network or ensuring the inter-operability of IT systems may require substantial resources)	7	14.9
There is insufficient commitment among target end-users to implement standards	8	17.0
There is insufficient commitment among target end-users to harmonise technologies, processes and procedures to promote inter-operability	17	36.2
Outcomes are unlikely to correspond sufficiently to end-user needs	5	10.6

5.7: What are the main benefits that your organisation expects to result from participation in PASR and FP7 Security projects? *Please identify the 3 most important reasons and indicate their degree of importance*

Benefits	Rank
The development of new knowledge and capabilities	1
The development of research and innovation	2
Strengthened cooperation and networking with EU and international partners	3
A better understanding of end-user needs	4
Strengthened cooperation and networking with EU and international partners	5
Greater visibility among potential end-user clients	6
Access to research centre of excellence	7
Consultancy and other opportunities to exploit knowledge and expertise	8
Multiplier effects (examples include knowledge-based projects leading to further research)	8
Other commercialisation spin-off effects	10
Strengthened competitive position in particular areas of EU Security Research	10
The opportunity to generate and exploit intellectual property	12
Access to future EU RTD Framework Programme funding	13
Access to national funding opportunities	14

5.8: To what extent do you believe that the project has achieved its objectives, or in the case of an ongoing project, is likely to achieve its aims?

Options	No	%
The project is likely to achieve its aims in full	33	45.8
The project is likely to achieve some but not all aims	28	38.9
The project is unlikely to achieve its aims	1	1.4
No response	10	13.9
Total	72	100.0

Full survey results

F

Is your organisation an SME?

Options	No	%
No	43	59.7
Yes	19	26.4

Non SMEs

6.1: To what extent have SMEs been involved in each of the following in your project?

Options	Major involvement		Some involvement		No involvement		Don't know		Total	
	No	%	No	%	No	%	No	%	No	%
Structuring the consortium at the bid stage	11	25.6	13	30.2	13	30.2	6	14.0	43	100.0
The preparation of the project application	14	32.6	17	39.5	8	18.6	4	9.3	43	100.0
Project management	5	11.6	12	27.9	20	46.5	6	14.0	43	100.0
Delivery of individual Work Packages	17	39.5	15	34.9	10	23.3	1	2.3	43	100.0
Conducting R&D activities	16	37.2	20	46.5	6	14.0	1	2.3	43	100.0
Carrying out knowledge-related activities	16	37.2	11	25.6	9	20.9	7	16.3	43	100.0
Dissemination activities	9	20.9	16	37.2	13	30.2	5	11.6	43	100.0
End user engagement	6	14.0	18	41.9	13	30.2	6	14.0	43	100.0

6.2: If intellectual property has been generated through your project, to what extent have SMEs been involved in:

Options	The generation of IP		The registration of IP and licensing arrangements		The exploitation of IP	
	No	%	No	%	No	%
Major role	6	14.0	5	11.6	5	11.6
Some role	5	11.6	4	9.3	5	11.6
Minor role	4	9.3	3	7.0	3	7.0
No role	6	14.0	8	18.6	7	16.3
No response	22	51.2	23	53.5	23	53.5
Total	43	100.0	43	100.0	43	100.0

SMEs

7.1: What is the size threshold of your enterprise?

Options	No	%
Micro (10 or fewer employees)	6	31.6
Small (10-50 employees)	7	36.8
Medium (50-250 employees)	6	31.6
Total	19	100.0

Full survey results

F

7.2: Which aspects of project implementation has your organisation (and any other SMEs taking part in the consortium) been involved in? (please tick all that apply)

Options	No	%
Structuring the consortium at the bid stage	11	57.9
The preparation of the project application	14	73.7
Project management	8	42.1
Delivery of individual Work Packages	14	73.7
Conducting R&D activities	15	78.9
Carrying out knowledge-related activities	14	73.7
Dissemination activities	10	52.6
End user engagement	9	47.4

7.3: How positively was the fact that your organisation is an SME viewed by other partners in the consortium during the initial partner search and consortium formulation stage?

Options	No	%
Very positively	4	21.1
Quite positively	9	47.4
Neutral	6	31.6
Negatively	0	0.0
Total	19	100.0

7.4 a): SMEs have a higher cost base than other partners (e.g. staff costs, general operating costs, R&D costs)

Options	No	%
Agree strongly	3	15.8
Agree to some extent	6	31.6
Disagree	8	42.1
Disagree strongly	2	10.5
Total	19	100.0

7.4 b): SMEs have been involved in delivering more cost-intensive Work Packages than other partners

Options	No	%
Agree strongly	6	31.6
Agree to some extent	7	36.8
Disagree	5	26.3
Disagree strongly	1	5.3
Total	19	100.0

Full survey results

F

Security Users Survey Response Tables

1.1: Which country is your organisation based in?

Country	N°	%
France	6	10.3
Germany	5	8.6
Spain	5	8.6
UK	5	8.6
Belgium	4	6.9
Denmark	4	6.9
Italy	4	6.9
Netherlands	4	6.9
European Union	3	5.2
Sweden	3	5.2
Croatia	2	3.4
Israel	2	3.4
Norway	2	3.4
Romania	2	3.4
Czech Republic	1	1.7
Greece	1	1.7
Luxembourg	1	1.7
Poland	1	1.7
Portugal	1	1.7
Slovenia	1	1.7
Turkey	1	1.7
Total	58	100.0

1.2 What type of user organisation are you?

Organisation	N°	%
Small or Medium Enterprise (SME)	5	8.6
Industry (other than SME)	5	8.6
University or Higher Education	2	3.4
Public research institute	12	20.7
National authority responsible for public health and safety / security	7	12.1
Regional or local public authority responsible for public health and safety / security	4	6.9
First responder, civil protection, ambulance or health services	5	8.6
Law enforcement and intelligence services - police, anti-terrorism bodies, customs and border control agencies	14	24.1

Full survey results

F

No response	4	6.9
Total	58	100.0

1.3 Which of the following priorities best describes the main areas of activity in which your organisation works ? (please tick a maximum of 2 boxes)

Options	N°	%
Increasing the security of citizens	32	55.2
Increasing the security of in frastructures and utilities	19	32.8
Intelligent surveillance and enhancing border security	13	22.4
Restoring security and safety in crisis situations	8	13.8
Improving Security Systems integration, interconnectivity	10	17.2
Security and Society	15	25.9
Security Research coordination and structuring	9	15.5

1.4 Have you been involved in an FP7 Security Research project either directly or indirectly?

Options	N°	%
Yes	42	72.4
No	16	27.6
Total	58	100.0

2.1 Which security research project(s) has your organisation participated in DIRECTLY as a formal member of a consortium?

FP7 projects	N°	PASR projects	N°
BIO3R	1	AMASS	1
ESSTRF	1	CPSI	1
EUROCOP	1	CRESCENDO	1
GATE	1	DECOTESSCI	1
IMPACT	2	DEMAST	1
ISCAPS	1	ESCoRTS	2
SECCONDD	1	EULER	1
SeNTRE	2	EU-SEC II	1
SOBCAH	1	FORESEC	1
STABORSEC	1	FRESP	1
TERASEC	1	Odyssey	1
TRIPPS	1	OPERAMAR	1
		SECTRONIC	1
		TALOS	3
		UNCOSS	1
Total	14	Total	18

Full survey results

F

Other projects you have been directly involved in

Other	N°	Other	N°
COMIFIN	1	INEX	1
ASTRO+	1	ISCAPS	2
BIO3R	1	LOTUS	1
BODE	1	NMFRD	1
CBRNEmap	2	Odyssey	1
COUNTERACT	1	OPERAMAR	1
CREATIF	3	Pandora	1
CRESCENDO	1	SECCONDD	1
CRISIS	1	SeNTRE	2
DEMASST	2	SMART-CM	1
DITSEF	1	SPIRIT	1
ESS	2	STACCATO	1
EU SEC II	1	STAR - TRANS	1
EUROCOP	1	TALOS	1
FESTOS	1	TRIPS	1
FRESP	1	Total	38

2.2 Has your organisation been involved in Security Research through participation as a user representative in projects (e.g. invited to take part in)?

FP7 projects	N°
I-TRACS	1
SeNTRE	1
SOBCAH	1
STABORSEC	1
Total	4
PASR projects	
AMASS	1
CPSI	1
CREATIF	1
EFFISEC	1
GLOBE	1
LOTUS	2
Odyssey	2
STRAW	1
TALOS	2
UNCOSS	1
WIMA ² S	1

Full survey results

F

Total	14
-------	----

Other projects you have indirectly participated in:

Other	N°	Other	N°
AQMASS	1	OPERAMAR	1
COMIFIN	1	SEABILLA	1
EFFISEC	1	SRC08	1
I2C	1	SRC09	1
INEX	1	SRC10	1
INFRA	1	TALOS	3
MoveON	1	WIMAAS	1
NMFRD	1	Total	0

2.3 How did you first become aware about the FP7 Security Research Programme?

Options	N°	%
Previous participation in the EU's RTD Framework Programmes e.g. FP6 and/or its predecessors	11	26.2
Word of mouth	1	2.4
Contacted by a consortium member in an FP7 Research Project	19	45.2
EU website on Security Research	1	2.4
National Contact Point	3	7.1
Research Executive Agency information day	0	0.0
Academic / research networks	1	2.4
Publication / news article	0	0.0
No response	6	14.3
Total	42	100.0

2.5 What has been your main role as a user or user representative in the project (please tick all that apply)?

DIRECT involvement (users that were formal members of project consortia)		
Options	N°	%
Member of (internal) user advisory group	7	16.7
Project design process – defining user needs	11	26.2
R&D activities - including the testing phase	13	31.0
Non R&D' activities (e.g. coordination, technical advice, etc)	2	4.8
Contributing to operational knowledge or procedures	8	19.0
Training activities	5	11.9
Activities relating to inter-operability and standardisation	6	14.3
Definition of future scenarios / foresight exercises	9	21.4

Full survey results

F

External user representative (i.e. users involved in projects but not formally part of the consortium):		
Options	N°	%
Member of (external) user advisory group	8	19.0
Project design process – defining user needs	6	14.3
External consultant to project	4	9.5
Participation in seminars and workshops	10	23.8
Activities relating to inter-operability and standardisation	2	4.8
Definition of future scenarios / foresight exercises	4	9.5

2.6a Was a formal advisory panel of users set up during the project?

Options	N°	%
Yes	17	40.5
No	17	40.5
No response	8	19.0
Total	42	100.0

2.6b How significant a role has the advisory panel played during the project's implementation?

Options	N°	%
Major role	8	47.1
Minor role	10	58.8
Minimal role	1	5.9
Total	19	111.8

2.7 How well did cooperation between users and other partners in the project consortium work during project implementation?

Options	N°	%
Very well	8	19.0
Quite well	18	42.9
Not well	0	0.0
Not at all well	0	0.0
No response	16	38.1
Total	42	100.0

2.8a Has your organisation made any use of research outcomes produced through the project(s) in which you participated to date?

Options	N°	%
Yes - considerable use	6	14.3
Yes - but limited use	9	21.4

Full survey results

F

No - too early in project	14	33.3
No - research results do not appear to be useful and relevant	0	0.0
No response	13	31.0
Total	42	100.0

2.8b If you indicated that you have already exploited project research results as a user, what were these?

Options	N°	%
Data	2	13.3
Products	0	0.0
Services	2	13.3
Technologies	1	6.7
Knowledge e.g. foresight studies, insights into particular areas of security research	15	100.0
EU-wide common minimum requirements and technical standards	2	13.3
Inter-operability of equipment, processes and procedures, IT systems	1	6.7

2.8d If you indicated that you have not exploited the research results, are you likely to do so in future, once the project has been completed?

Options	N°	%
Definitely, even if this means investing our own resources (e.g. through procurement).	3	21.4
Probably, but only if the project outputs can be exploited free-of-charge	3	21.4
Probably, but only after the research has been further developed	6	42.9
Unlikely	0	0.0
Definitely not	0	0.0
Don't know - it is too early in the project to determine how useful the research outcomes will be to users	2	14.3

2.9 Overall, how relevant to user needs are the research outcomes that have been carried out through the project, from your perspective?

Options	N°	%
Highly relevant	10	23.8
Quite relevant	14	33.3
Not that relevant	4	9.5
Not relevant at all	0	0.0
No response	14	33.3
Total	42	100.0

Full survey results

F

2.10. Which aspects of the project has your organisation been able to contribute most added value to in terms of user input? (please tick a maximum 2 choices)

Options	N°	%
Testing user requirements	7	16.7
Operational knowledge or procedures	13	31.0
R&D phase	8	19.0
Testing phase	3	7.1
Future scenario development/ foresight	13	31.0
Advice / guidance on the ethical aspects of security research	2	4.8

2.11 Overall, how satisfied are you with your participation in an FP7 SEC project in terms of:

Options	Your general expectations		The quality and usefulness of the results produced through the project research	
	N°	%	N°	%
Highly satisfied	9	21.4	7	16.7
Quite satisfied	15	35.7	15	35.7
Not satisfied	4	9.5	3	7.1
Not satisfied at all	0	0.0	1	2.4
No response	14	33.3	16	38.1
Total	42	100.0	42	100.0

2.12 Have you drawn the attention of any other user organisations to the research project?

Options	N°	%
Yes	25	59.5
No	1	2.4
No response	16	38.1
Total	42	100.0

2.13 Do you perceive there to be any barriers to the uptake of research results developed through EU Security Research projects from an end-user perspective? (please tick any that apply)

Options	N°	%
The results of the research are potentially useful, but only after further development	14	33.3
Results will only be exploited by users if these are free-of-charge	4	9.5
There would be prohibitive costs in using the research results	2	4.8
There are practical difficulties in implementing a harmonised EU approach in our area of security	11	26.2
There are practical difficulties in promoting inter-operability	7	16.7

Full survey results

F

There are no particular obstacles	2	4.8
-----------------------------------	---	-----

2.15 Have you participated in any nationally funded Security Research programme(s)?

Options	N°	%
Yes	14	33.3
No	14	33.3
No response	14	33.3
Total	42	100.0

If 'No' in Q1.4

3.1 Have you heard of the FP7 Security Research Programme?

Options	N°	%
Yes	12	75.0
No	3	18.8
No response	1	6.3
Total	16	100.0

3.3a What types of research results would be most helpful in meeting the security challenges you identified (please tick ALL that apply)

Options	N°	%
Data	4	33.3
Products	5	41.7
Services	3	25.0
Technologies	8	66.7
EU-wide common minimum requirements and technical standards	6	50.0
Inter-operability of equipment, processes and procedures, IT systems	9	75.0
Knowledge and good practice guidance e.g. foresight studies, insights into particular areas of security research	9	75.0

If you ticked any responses above, please provide information on the types of research results, knowledge and tools that could be most relevant in meeting the current challenges that you face in the security field

Data
Collecting data is fundamental for identification of security issues. We need to be capable to gather all significant data in an automated system connected to other security systems.
Facts on impact of security measures and censorship
Products
First responders training
We need high-tech products that are capable of meeting our needs for scanning vessels, containers, underwater areas, automated data gathering and data mining systems, all inter-connected and efficient.
Services
inter-exchange of experts border cooperation
Technologies
Mobile, fast neutron scanners for vessels and containers, chemicals detecting systems, thermal imaging scanners

Full survey results

F

interconnected with other security systems and other IT systems within port.
Encryption Anonymity enhancing technologies.
Knowledge e.g. foresight studies, development of databases containing knowledge repositories in particular areas of security, insights into particular areas of security research
Very important.
EU-wide common minimum requirements and technical standards
Fire prevention in buildings
Inter-operability of equipment, processes and procedures, IT systems
Most important.
Processes to support counter-terrorism
Other
The External Integrated Surveillance system is used mainly to fight against trans-border criminality, trafficking in human beings, trafficking in drugs. It is composed for radar systems, optronic systems and communications.
Human behaviour in crisis situations

3.4 To the extent that you are able to comment, do the types of activities being supported through FP7 Security Research appear likely to meet your needs as a prospective user of research outcomes?

Options	N°	%
Yes, strongly	0	0.0
Yes, to some extent	8	50.0
To a limited extent	6	37.5
Not at all	0	0.0
No response	2	12.5
Total	16	100.0

3.5 To what extent is there scope for the development of common EU minimum technical standards in the area of security in which your organisation works?

Options	N°	%
Strong scope	3	18.8
Some scope	4	25.0
Limited scope	6	37.5
No scope	0	0.0
No response	3	18.8
Total	16	100.0

3.6 To what extent is there scope for greater inter-operability (for example, in IT systems equipment, processes and procedures) in the area of security in which your organisation works?

Options	N°	%
Strong scope	4	25.0
Some scope	6	37.5
Limited scope	2	12.5
No scope	0	0.0
No response	4	25.0
Total	16	100.0

Full survey results

F**3.7 Have you participated in any nationally funded Security Research programme(s)?**

Options	N°	%
Yes	2	12.5
No	12	75.0
No response	2	12.5
Total	16	100.0

National Security Research Programmes

G

National Security Research Programmes

As part of the evaluation research, an analysis of National Security Research Programmes was undertaken. The aims of the research were to:

- Assess the extent to which at national level, civil security research programmes are being supported by the Member States;
- Compare the level of funding available at national and EU level for such programmes;
- Assess and compare the aims and thematic focus of national programmes and whether there is complementarity in terms of objectives and priorities with the ESRP
- Examine the extent to which the ESRP complements National Security Research Programmes (and vice versa);
- Consider whether the launch of a European Security Research Programme has had any influence in encouraging the Member States to invest in Security Research at national level and in the development of a strategic policy framework to facilitate this;
- Identify differences between national programmes and ESRP (e.g. eligibility by organization type, whether funding schemes allow any scope for transnational cooperation);
- Obtain the views of beneficiaries on their experiences of taking part in the ESRP and National Security Research Programmes (e.g. ease of access to funding, monitoring requirements, etc.; and
- Draw conclusions on the extent to which the ESRP demonstrates Community Added Value.

The starting point was to identify EU countries that fund National Security Research Programmes. There are currently **only seven EU countries that fund national security research**. The main National Security Research Programmes and strategies identified include:

- France: Research Programme CSOSG - Concepts, Systèmes et Outils pour la Sécurité Globale (National Research Agency ANR)
- Netherlands - R&D Programme on Security, Safety and Technology
- Sweden - National Security Technology Research and Innovation Programme
- Finland - Technology Programme on Safety and Security
- UK – a number of programmes, including the UK CBRN Resilience Programme
- Austria - KIRAS – the Austrian Security Research Programme
- Germany - Research for Civil Security Programme

Some national programmes focus mainly on R&D, such as the federal programme in **Germany** which is implemented with support from regional state Lander. In other countries, such as **Finland**, there is a focus on both R&D and on promoting cooperation between suppliers and users of security products, services and solutions and improving coordination within the user community.

In the **UK**, there are multiple programmes, coordinated through an overarching security research strategy, the Security and Counter-Terrorism Science and Innovation Strategy. There are then a number

National Security Research Programmes

G

of funding pots that support different aspects of security research. Some are more R&D and technology focused, such as the UK CBRN Resilience Programme, while others focus on carrying out social research and community and law enforcement engagement to combat extremism and radicalisation (e.g. Prevent Programme).

Funding

With regard to funding, among the findings were that national security research programmes have a relatively small funding allocation compared with the ESRP, and this has implications in terms of progress towards strengthening the competitiveness of the security industry in Europe, given that a central programme aim is to help develop critical mass, and to reduce the industry's fragmentation.

While it was not possible to obtain detailed funding information from all countries, selected examples were obtained. It is worth pointing out that in some countries, such as the UK's Ministry of Defence, while funding is provided for civil security research, since funding may be within a much broader envelope, it is difficult to disaggregate the civil security research component.

Examples obtained include **Germany**, which has allocated €129m or €43m per year for the implementation of its Research for Civil Security Programme, which is being implemented by the Federal Ministry for Education and Research (Bundesministerium für Forschung und Entwicklung – BMBF in the period 2008-2010. This is broadly similar in terms of budget to that of the **Austrian Security Research Programme**, which has been allocated €110m. In the UK, it has proved more difficult to obtain comprehensive data on funding allocation, mainly because funding is split between a number of separate programmes, which feed into an overarching strategy. Some data was obtained however. For example, in the **UK**, the CBRN Resilience Programme has a budget of 10m, which forms part of the UK strategy on combating terrorism CONTEST, has a budget of 12.5m.

In **Finland**, the Tekes Safety and Security Programme being implemented by the Finnish Funding Agency for Technology and Innovation (Tekes) has a budget of €160m. Sweden has also recently decided to fund a national programme, with 120m Swedish krona of funding.

While such funding programmes represent a significant opportunity for the security industry (both SMEs and large firms), comparatively, FP7 SEC provides very significantly funding opportunities for cross-border collaborative research and for larger-scale demonstrators. FP7 SEC was therefore seen by those responsible for managing national programmes as a major source of research funding not only in countries that do not presently have a national Security Research Programme, but given the comparatively modest funding scale, also in countries that do operate such programmes.

Thematic focus

In terms of research themes supported, there was a large amount of cross-over between EU and national security research programmes. Among the most common themes addressed include:

- Aviation security
- CBRNE
- Crisis management / emergency response
- Critical infrastructure protection
- Land border and maritime security

National Security Research Programmes

G

- Networked systems, interconnectivity and interoperability
- Strengthening cooperation between counterparts in other EU countries (increasing cross-border aspects to internal security)

The focus on similar priorities reflects the fact that there are broadly common priorities for all Member States in protecting the security of citizens from terrorism, in protecting critical infrastructure, and in ensuring that EU external borders (land, maritime) are protected, and that crisis management processes and procedures and equipment are made more interoperable, among other priorities.

There were some differences in some national programmes. For example, in Finland, there was a stronger emphasis on environment security and on improving security at regional level than in FP7 SEC. The research also found evidence that the Member States are increasingly concerned about cross-border security issues. However, there has so far been limited interaction between national programmes in the most important areas of scientific and technological research. Some cooperation was identified, for example, between the national programmes in Germany and Austria.

Some themes within ESRP appear to have been given an especially strong focus among national security research programmes such as CBRN. There is a strategic difference between some Member States regarding the level threat from CBRN and the amount of resources available to prepare, prevent and respond to CBRN attacks. It is notable that while the UK, French and German programmes are largely focused on mitigating CBRN threats, this theme has comparatively less focus in the Swedish and Austrian programmes. The ESRP can also be seen as having played a vital role in providing security coverage for Member States that do not have their own national programme, and who would otherwise have less tools at their disposal and research results to address the growing threat posed by malevolent use of CBRN.

Types of organisations taking part in National Security Research Programmes

The types of organisations that have been involved in national programmes were examined. The findings were that broadly similar research actors are involved at the national level in security research projects as at EU level. Indeed, many are involved in both the national and EU levels.

For example, in Germany, according to one interviewee, a 'wide variety of actors are involved in the R&D security programme: private companies, public universities, publically funded research institutions such as the Fraunhofer Gesellschaft and several Ministries (Defence, Interior, Economy, Education).

User involvement in National Security Research Programmes

The ESRP strongly encourages the active participation of users in the programme. The extent to which users have been involved in national programmes was therefore examined.

Although national programs have been successful in establishing greater cooperation among industry stakeholders and end-users at the national level, there are a number of weaknesses that result from pursuing a national approach to scientific research, especially in the context of transnational threats that affect more than one country. Furthermore, national programmes are designed to represent a more politicised set of priorities which often translates into a narrower focus for project research.

In common with FP7 SEC, some national programmes put a strong emphasis on user involvement. For example, a number of **Finnish** public end-users are participating in the Finnish Safety and Security Programme. These include national Ministries (e.g. Social Affairs and Health, Transport and Communications, Environment, Foreign Affairs, Justice, Interior), public agencies (e.g. Radiation and

National Security Research Programmes

G

Nuclear Safety Authority, National Emergency Supply Agency), transport authorities (e.g. Finnish Vehicle Administration and Finnish Rail Administration, Civil Aviation Administration) and city authorities (e.g. Helsinki, Espoo, Turku). Users appear to have been closely involved in Innovation Networks focusing on particular themes e.g. Supply Chains, IT Security, Crisis Management and Rescue, CBRNE, Command and Communication.

The involvement of users in the KIRAS Programme in **Austria** was mandatory for every project that was supported. Users were involved in the process of developing the KIRAS programme, including research institutions, applied science laboratories and leaders of industry. Priorities in the civil security sphere are generally determined by political institutions in Austria. For this reason the projects were driven by political specifications and public procurement measures. Therefore public consumers such, as the Ministry of the Interior and blue light organisations, have received strong government support under the KIRAS programme. Austria aims to create competitive economies of scale in the area of security by harnessing the innovation and skills of its scientific research community.

Ease of access to research funding

One of the issues examined was how easy it was for beneficiaries to access security research funding through national programmes, and how this compared to ESRP. Different aspects were assessed, such as the overall ease of access, the efficiency and timing of the application and contracting process and monitoring and reporting requirements.

Among the comments made by interviewees in the UK and Germany (companies, national authorities and industry associations on the supplier side) were that while the EU RTD programmes are attractive and provide an important source of research funding, there are concerns that FP7 decision making procedures and time to grant are too long and bureaucratic. This was seen as applying not only in FP7 SEC, but across the Cooperation Programme and in previous RTD FPs.

In Germany, an interviewee from the Ministry of Interior in Brandenburg Land, stated that the German national security programme is simpler and the application form is shorter (20 pages). Industry and SMEs were said to view taking part in the national programme as more straight forwards and imposing less of an administrative burden than the EU RTD FPs. Consequently, the number of beneficiaries in the German national security research programme is higher than the number of German firms taking part in FP7 SEC. The need to simplify procedures was seen as particularly important in enabling SMEs to access security research funding.

Discussions in the UK with industry suppliers and some departments within UK government, such as the Home Office found that while there was strong support for the added value of a European Security Research Programme, there was a concern that the lead times in getting projects underway were not as quick and responsive to identified need as national funding. For example, both in defence and civil security research, it is common for small amount of 'seed funding' to be made available to carry out small pieces of research to develop initial project ideas and to test proof of concept. The procedures involved in applying for such funding are straight forwards and only require a short project brief / proposal to be prepared. FP7 SEC while useful, was seen as being more administratively difficult to access funding and to fulfill reporting requirements.

This was also seen as deterring users from being more actively involved in the programme. The overall perception was that domestic funding is easier to access because it is less administratively burdensome. Some of the comments came from prospective rather than actual beneficiaries in FP7 SEC – but is useful to note this external perception.

National Security Research Programmes

G

Impacts of the ESRP on national programmes – and vice versa

The ESRP has had various positive impacts at the national level. First and foremost, it has promoted **stronger cooperation** on security research matters between relevant actors (both nationally and in terms cooperation with counterparts in other EU countries). This has been achieved both at the programme level (for example, through the setting up and regular meetings of the Security Programme Committee) and at the project level in specific areas. An example was the EUSEC II project, which brought together police forces and Ministries of Interior from 22 countries to discuss common approaches and to develop more effective practices in security planning for major events.

The ESRP has also influenced the national debate on the extent to which it is necessary post 9-11 to provide funding for civil security research programmes, rather than relying on defence spending alone to protect citizens. While the level of policy attention and funding to civil security research has been increased as a result of terrorist attacks, including those in London and Madrid, the ESRP has had a direct role in encouraging more Member States to fund civil security research.

For example, **Germany** explicitly set up its own national civil security research programme in response to the Commission's decision to fund the ESRP. This was partly because there was a willingness to strengthen investment in this area to improve national capabilities and preparedness, but a key aim of the programme is also to provide funding to encourage the development of research excellence among security research actors so that they are able to participate in collaborative transnational research through ESRP. This is a very good example of how national funding programmes can serve as a de facto seed fund to help develop capacities in areas of relevance to priorities outlined at the EU level. In this way, funding and research synergies between national and the EU SRP are beginning to be leveraged.

In **Lithuania**, the discussions with the NCP suggest that while there is presently no national security research programme, in order to help structure the market, and to encourage participation in FP7 SEC, there could potentially be funding to set up a small programme in future.

The research also identified a small number of firms that have already used experiences gained from their participation in PASR and FP7 Security projects to **leverage further funding through security research programmes at national level**. For example, a partner in the **SecurEau** project, the Finnish National Institute for Health and Welfare, which specialises in applying microbiology research to the field of safety and security, was involved in the development of secure drinking water distribution systems following deliberate contamination. The experience and knowledge gained through the project was seen as being very valuable by this organization and there is an intention to capitalise on the knowledge gained through a possible follow-up project. The Finnish Technology Programme on Safety and Security was particularly interested in supporting projects in this area and some Finnish end-users have expressed a strong interest in research to ensure the security of water supplies.

In the **UK**, a good example was identified of ways in which national security research funding programmes can serve as a springboard and initial building block to then carry out further research and development. For example, the **iDetecT4ALL project** is developing a novel photonic sensor technology based on ultra low cost electro-optical components and using a single sensor for the detection and authentication of objects. An initial development project was funded at national level, but funding was not available on a sufficient scale for the necessary further development from this source. FP7 funding is allowing the company to take the development of the technology through a proof of concept to the point where it will be in a position to raise investment funds for production and marketing.

National Security Research Programmes

G

Scope for transnational research

Most national security research programmes examined are domestically focused. However, in **Germany** and in **Austria**, there is some scope for collaborative research on a transnational level

The transnational elements of the ESRP was viewed by national security research stakeholders as providing a real added value, given that the European security market suffers due to the fragmentation of research markets according to national priorities. This fragmentation has a negative impact on the competitiveness of the European security market and means some areas lack a critical mass to be globally competitive. Where security themes overlap the national research programs are not always effective in establishing the cooperation necessary to prevent duplication. Therefore many projects at the national level do not fully exploit potential partnerships with other Member States which leads to a lack of complementarity in the development of new technologies.

A key benefit that research at the EU level brings is that niche technical capabilities can be leveraged from a broader group of Member States.

Detailed overview of National Security Research Programmes

Germany: The Research for Civil Security Programme

In Germany, the Federal Ministry for Education and Research (Bundesministerium für Forschung und Entwicklung - BMBF) is responsible for security research. Following a consultation process which involved workshops to develop a national strategy on Security Research, a national security research programme was adopted by the BMBF. Funding on security research began in early 2007 with expenditure of €43m per year over a 3 year period.

The BMMF defines the key aims of the programme in its strategy document “Security research - research for the protection of society”⁴. “The BMBF's security research program ‘Research for Civil Security’ aims to increase civil security as well as preserve human rights and civil liberties. The results are expected to contribute towards early warning of threats to civil security by identifying the main causal dangers. The results will also enable government and user organizations to take efficient countermeasures and develop efficient forms of organization as well as technical means of preventing threats such as terrorist attacks and managing crisis situations.

Types of intervention

With regard to the types of interventions eligible for support, the programme is divided into two lines of supportive action. Program line-1 is comprised of scenario orientated research based on the problem solving perspectives of end-users and is geared towards improving collaboration between authorities and private operators of security related infrastructure. The core elements of the support include protection and rescue of people, protection of transport infrastructures, protection against failure of the supply infrastructures, and securing the supply chains. The first line encourages the development of a community of market stakeholders rather than focusing on individual technological results.

Program line-2 supports technology interconnections that can be applied across all security scenarios. These include technologies for rapid and reliable identification of persons, rapid and mobile identification of hazardous substances, pattern detection and boosting deployments of security and

⁴ Source: <http://www.bmbf.de/en/6293.php>

National Security Research Programmes

G

emergency services. The technology interconnections utilise relevant technological knowledge of security research to help develop innovative systems from existing and new technologies. The program intends to apply technology interconnections at the application level involving the entire research innovation chain from industry to end-users.⁵

Programme structures and development

The security research programme is based on an analysis of the causes of insecurity (e.g. radicalization in Germany, potential threats and gaps in the security of infrastructures) carried out in the respective policy areas of government departments. It also allows new types of threats, causes and future security requirements to be addressed in interdepartmental plans. While the federal government controls the strategic direction of the security research programme, there is strong support for cooperation among various government departments.

Cooperation takes place between security research and other research programs being implemented by the Federal Ministry of Education and Research. For example, in technology research, life sciences, earth system research, the humanities and social sciences, cooperation has been strengthened between relevant research and policy departments. Similar cooperation structures are being shaped in other areas of German research at the national level, such as:

The Federal Ministry of the Interior (responsible Germany's domestic security in relation to protection against terrorism and crime, protection of critical infrastructures, protection of the population and, in the event of disaster, IT security and the reinforcement of emergency services) and the Federal Ministry of Transport (responsible for building and urban affairs in relation to structural protection, the Galileo satellite navigation system and the securing of traffic and transport.

In addition, the security research programme is helping to fuse environmental aspects of security research such as environmental protection and nature conservation, nuclear safety, and air and space travel, that are implemented by the Federal Ministry of the Environment in cooperation with the Federal Ministry of Economics and Technology, with overlapping research into bioterrorism, epidemics and pandemics, which are being supported by the Federal Ministry of Food.

Stakeholder and user involvement

The security technology market in Germany is highly developed with significant cooperation between the public and private sector. In 2005 the German security market was worth EUR 10 billion and its global growth is 7-8% per annum. The German security research market is focused holds a competitive advantage in areas such as micro-systems technology, optical technology and sensors. Germany's national security research programme is also closely integrated with FP7 security research undertaken at the EU level, which improves the market conditions for German companies competing at the international level.

A wide variety of actors are involved in R&D security matters in Germany: private companies, public universities, publically funded and co-funded research in non-university institutions such as the Fraunhofer Gesellschaft and several Ministries (Defence, Interior, Economy, Education) are also involved. In addition the BMBF sponsored three workshops named, 'Security Research: Development of a National Strategy' which brought together a large number of experts from different areas of the security market.

⁵ BMBF: Research for Civil Security: Programme of the German Federal Government.

National Security Research Programmes

G

The workshops played an important role in defining the needs of the programme as seen by security industry on the supplier side and end-users on the other. Overall three workshops took place to help outline the views of researchers on which technologies demonstrate the most growth potential as well as joint scenario definition exercises between researchers and end-users to help match technologies with particular needs.

Austria: KIRAS –Security Research Programme

Austria was one of the first EU Member States to develop a national security research programme. The Austrian government has allocated a total budget of 110 million Euros in direct subsidies to the programme for the period 2005-2013. The concept for the programme is based on the etymology of the Greek work KIRAS, which is made up of the words "kirkos" (circle) and "asphaleia" (security). The circle has to be understood as representing the holistic concept behind, because in the programme. Austria has a strategic objective to integrate the activities of KIRAS with the European Security Research Programme.

At the same time, partner countries, such as Germany, are positioning their security research programmes to increase collaborative cooperation with the KIRAS. From its inception the KIRAS programme gave priority to the protection of critical public infrastructures. The threat of terrorist and sabotage is highlighted as one of the main concerns as well as natural disasters and the consequences of serious industrial accidents. The aim of the programme is to ensure the continuation of the basic functions of the state and the resilience of the population in the event of large scale threats to human life.

Overall the programme has set itself six strategic **objectives**, which include: the creation of knowledge that is required for the achievement of the security-political objectives of Austria; increasing of the objective security and the subjective security perception of the population; developing relevant and new security technologies; growing the security industry; building up excellence in security, and integrating the relevant social and socio-political questions with all projects.

Types of intervention

The KIRAS programme in Austria employed a broad approach to the selection topics. In principle only civilian research is supported, however some projects also include the design of goods which can be used for both civilian and military purposes such as explosives detection, biometrics and special IT solutions. KIRAS is based on four programme lines, which complement each other:

- Programme Line 1 ("Networking and Probing") promotes networking at national level as a means of maximising resources and expertise as well as technical feasibility studies
- Programme Line 2 ("Cooperative R& Projects") aims at transferring newly acquired knowledge into applied research and technology development
- Programme Line 3 ("Component Development and Demo Projects") checks the appropriateness of innovative ideas, concepts, technologies and systems in the field of security research
- Programme Line 4 ("Accompanying Measures") support the other three Programme Lines with studies, for example⁶

⁶ Security Research: Austria Innovativ. Federal Ministry of Transport, Innovation and Technology. 2010

National Security Research Programmes

G

KIRAS focuses on developing prototypes into products that can be marketed to the public, purchasers and users. In the first Call for Programme Line 2 (December 2006 until February 2007) 48 projects with a total volume of about 30 million Euros were submitted. Almost 500 jobs were created. Although the programme has been in operation for a relatively short time KIRAS is already among the leading countries at European level, in terms of making inputs to the ESRP. All projects are either complete or on schedule to achieve all their results and intended outcomes.

Programme structures and development

KIRAS was developed by the in coordination with the Council for Research and Technology Development (FFG). While the Federal Ministry of Transport, Innovation and Technology (BMVIT) is responsible for determining the KIRAS structure, strategy and financing. The role of the FFG is to provide overall programme management. The programme launched a Call for Expressions of Interest in 2005 which received strong response including the submission of over 250 project applications. Initially the programme experience high rates of over-subscription, which was partly due to the FFG's support for consultation, proposal checks and Presenter's Day workshops.

The FFG provides consultation to potential stakeholders to assist their choice of promotional programmes, to improve their awareness about international cooperation projects, and increase their access to activities in space and especially in the cooperation of science, the economy and the application of research results. The FFG plays an important role in coordinating activities under the KIRAS programme, although operating bodies are divided between the BMVIT and the Federal Ministry of Economics and Labour (BMWA). Being a supplier of promotion services the FFG also operates by order of other national and international institutions.

Programme managers designated a jury of experts to communicate a detailed statement of reasons where projects proposals failed. The detailed statement not only provides the reasons for failing, but also shows how the application can be improved for the next submission. This is an adjustment and learning process for the companies participating in KIRAS. The sustainability process is also confirmed by the fact that initial difficulties, such as wrong priorities set in the applications or unclear explanations in the scientific part, have largely been eradicated. A strong emphasis is placed on making applicants conform to ESRP criteria and standards.

Stakeholder and end-user involvement

The humanities, social sciences and cultural studies (HSC) feature prominently in a large number of KIRAS projects. The decision to include HSC was taken to address issues such as interference with basic rights and the privacy of citizens. By minimising these risks Austria has helped integrate of HSC involvement in the ESRP. Wedded to this is a high degree of practical and economical orientation across the programme which improves the potential for end-user and outside industry participation in projects. KIRAS has demonstrated a high quota of successful applications by Austrian companies, universities and extramural research facilities. This has prepared them for participation in the ESRP, which is a significant benchmark for many national stakeholders.

Finland: Technology Programme on Safety and Security

The Technology Programme on Safety and Security in Finland is being implemented through the Finnish Funding Agency for Technology and Innovation (Tekes) (Tekes). The programme aims to create commercial security solutions for international markets by providing funding for innovative and corporate security research projects. The objective of the applied research is to offer services that

National Security Research Programmes

G

support international co-operation and market entry for Finnish companies. The programme is being carried out between 2007-2013 and has a total budget allocation of €160 million of which Tekes manages €80 million. There are currently over 200 companies participating in the Finnish security research programme. Tekes has launched a technology programme that will help Finnish enterprises and researchers develop international business activity and competence in safety and security technologies, services and solutions. The programme aims to grant €80 million for new projects over a seven year time frame.

The programme is divided into 3 parts: National safety and security which addresses border guards, police, first response and fire fighting as well as customs operations, Industrial safety and security deals with the full agenda of corporate needs and respective solutions and Citizens safety and security. By the end of 2009 the programme had funded more than 90 projects with total funding amount of €54 million. Over 180 Finnish enterprises are involved in the Programme including a large number of Safety and Security authorities.

Types of intervention

Tekes supports security research in three areas where there is the greatest need for the design of new technologies and applications, these include:

National Safety and Security

- Public procurement procedures
- Equipment and solutions for fire and rescue, police, crisis management, border security, maritime safety and security, critical infrastructure protection
- Market entry prerequisites and restrictions

Corporate Safety and Security

- Business to business – market
- Equipment and solutions for supply chain security, industrial safety, fire protection, cyber security, occupational safety, access control, identification

Consumer Safety and Security

- Business to consumer-market
- Also public procurement by social sector
- Home solutions, independent assisted living for seniors
- Cultural values, acceptance, privacy issues

Funding is primarily allocated for Finnish companies which carry out R&D.

In addition to funding the programme organizes a number of other services such as:

- Studies & surveys – markets, trends, legislation - which cover selected countries and customer segments
- Workshops to help actors within the safety and security branch to network and to develop joint project initiatives

National Security Research Programmes

G

- International networking and match making events in all continents

Stakeholder and user involvement

International co-operation is an essential part of Safety and Security development in Finland. Safety and Security programme actively builds international connections and provides support for international activities for Finnish researchers and companies. Tekes also requires that the research projects involved in the programme foster international researcher mobility. The three areas of intervention under the Tekes programme allow a wide scope for public and private sector end-users to become involved in delivering project results.

United Kingdom: Science and Technology Strategy for Countering International Terrorism

The UK faces a sustained terrorist threat which is reflected in the orientation of its support for security research activities. In 2007 the Home Office established an internal department named the Office of Security and Counter Terrorism (OSCT) together with the Home Office Scientific Development Branch (HOSDB). Their role is to support the implementation of the UK's Strategy for Countering International Terrorism (CONTEST) and to work with industry stakeholders to deliver the UK's Science and Technology Strategy for Countering International Terrorism. In 2008, the cabinet office set up the Strategic Horizons Unit to coordinate all government related horizon/foresight scanning work, including science and technology.

One of the key strategic objectives is to ensure security and resilience for the public, economy, infrastructure, territory and UK way of life from all major risks that can affect the country directly – requiring both direct protection against real and present threats such as terrorism and cyber attack, resilience in the face of natural and man-made emergencies and crime, and deterrence against less likely threats such as a military attack by another state.⁷

Types of intervention

Government funding for security research aims to address the challenges set out in relation to each of the CONTEST strategies four main work streams (i.e. *Pursue*, *Prevent*, *Protect* and *Prepare*). These challenges will be addressed by scientific and technological inputs in the following areas:

- Understanding the causes of radicalisation
- Protecting national infrastructure
- Reducing the vulnerability of crowded places
- Protecting against cyber terrorism
- Improving analytical tools
- Identifying, detecting and countering novel and improvised explosives
- Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive threats (CBRNE)⁸

⁷ A Strong Britain in an Age of Uncertainty: The National Security Strategy. Cabinet Office. UK. 2010

⁸ The United Kingdom's Science and Technology Strategy for Countering International Terrorism. Directorate of the Home Office. UK. 2009

National Security Research Programmes

G

Programme structures and development

The OSCT is also leading the cross departmental programme, INSTINCT, which aims to “enable government to make the most of innovative projects and ideas in counter-terrorism by providing a greater understanding of the innovation community, smarter influence over external innovation and better coordination investments in new ideas and solutions”. The INSTINCT programme includes calls for proposals on a variety of topics relevant to counter-terrorism.

The organisations involved in INSTINCT include the Defence Counter-Terrorism Science and Technology Centre (MOD CT Centre), the Centre for the Protection of Critical National Infrastructure and the Association of Chief Police Officers (ACPO). In addition the Ministry of Defence’s Centre for Defence Enterprise (CDE) is the first point of contact for organisations with a disruptive technology, new process or innovation that has a potential defence application.⁹ Through RISC five joint Industry Advisory Groups have been established in areas of particular importance to the needs of UK security research:

- Chemical, Biological, Radiological and Nuclear (CBRN)
- The Critical National Infrastructure (CNI)
- Information and Communication Technology (ICT)
- Detecting suicide bombers
- Olympics

RISC has also identified a number of common themes between UK security research and recent calls for proposals in under the FP7 European Security Research Programme:

- Countering Improvised Explosive Devices (IEDs)
- CBRN Protection (UK research in this area)
- Airport Checklist Screening
- Cyber attacks against critical infrastructures
- Security of biometric data and travel documents
- Artificial sniffer (screening)
- Operational data exchange (i.e. knowledge management)
- Best practice for security in urban zones (i.e. crowded places)
- Effective approach between end-users and SME’s

Stakeholder and end-user involvement

The UK government has a long track record of working with the science and technology industry across the military, security and intelligence markets. OSCT works with industry through a variety of routes including trade associations, exhibitions, industry primes and the Technology Strategy Board.

⁹Countering the Terrorist Threat, Ideas and Innovation: How Industry and Academia can Play Their Part. Directorate of the Home Office. 2009

National Security Research Programmes

G

The main stakeholders in UK security research include the Security and Resilience Suppliers Community (RISC) and INTELLECT which represents the UK technology industry. RISC is an alliance of suppliers, trade associations and academics representing over 2000 companies ranging from prime contractors and global leaders through to SME's and start ups.

The Science and technology strategy also aims to support SME's with strong records in creating innovation. The OSCT works with industry and academia through other routes such as liaison, responding to inquiries, networking at conferences, exhibitions and events through exploring opportunities in existing science and technology projects.

Sweden: National Security Technology Research and Innovation Programme

In Sweden, the Civil Contingencies MSB is responsible for implementing the National Security Technology Research and Innovation Programme. Through this programme the MSB aims to inspire new ideas and focus research on important fields of knowledge in the field Civil Contingencies. The research program is primarily aimed at researchers with an interest in the issues that fall within the field of Civil-security and preparedness.

The programme will be implemented over the period 2011-2013. The programme has a budget of 120 million Kronor. Further direction of research is the basis of detailed documentation and mapping of skills needs.

Research will be targeted on specific security topics and issues that are identified as priorities by the Swedish government. The objective of the research program is to provide a platform for interaction between various stakeholders, government, industry and research organizations. Interaction between academia and the surrounding society is pursued in order to effectively solve practical problems and exchange knowledge and best practice within the security research community.

Types of intervention

For the period 2010-2013, the MSB highlighted six areas in which national Authority's should concentrate their activities. Other activities to be carried out by different agencies during the program period, but their focus will contribute to the common goals set by the MSB. The areas of focus will also be the basis for the priorities of the research that the MSB decides to fund, these include:

- Dealing with the consequences of a changing climate
- Taking advantage of societal resources
- Developing requirements for managing and coordinating security projects
- Developing local cooperation with the Civil Preparedness agencies
- Developing MSB's capacity to contribute towards security objectives
- Clarifying objectives, responsibilities and dependencies

Programme structure and development

The role of the Swedish Security Research Programme is to ensure that research is relevant to the six security priorities assure the quality of research. The Authority is responsible for communicating research results to different audiences supporting the implementation of the programs vision and objectives.

National Security Research Programmes

G

The security programs mission and goals incorporate the principles governing criteria for funding, collaboration and communication. The security program also details the modalities for research funding. The programme is also designed to prepare the public for crisis situations under the mission title "A safer society in a changing world". The programs overall goal is to reduce the risks of accidents and emergencies, to develop and support society's collective preparedness, and to reduce the impact of disasters when they occur.

The programme has been extended to include activities to help safeguard the life and health, the functioning of society, and ability to maintain the fundamental values of democracy, the rule of law and human rights and freedoms. To support these areas the MSB is responsible for activities relating to actions before, during and after a crisis. The mission spans the entire threat and risk spectrum, from everyday accidents, serious incidents, crises and heightened state of alert. MSB will be proactive in the process of prevention and vulnerability reduction measures. In order to strengthen community protection and preparedness, some projects look at how society responds to crisis and what can be done to improve existing procedures for responding to emergencies.

Stakeholder and user involvement

MSB's work spans multiple sectors of society and industry. Therefore the MSB has developed strong cooperation with other agencies, businesses, and universities. Work is conducted largely through the various networks of representatives. By arranging joint calls with other authorities the MSB has increased the impact of research funds. There is high degree of overlap in terms of the security challenges faced by other Nordic. Research agreements have been established between Sweden and other Nordic authorities to promote a Secure Society and establish common Civil Contingencies. It is believed that this cooperation will strengthen the position of Nordic countries science and technology companies within the EU and internationally.

MSB promoted Sweden's successful participation in the ESRP as well as in similar research programs in the USA. MSB is also responsible for coordinating national efforts within the framework of existing Agreements between Sweden and the Department of Homeland Security (DHS), USA. The overall objective of the agreement is to initiate and promote sustained interaction between the MSB and the DHS, the Swedish authorities and their counterparts within DHS-sphere. Swedish public and private research providers have established a close with US based security firms.

The Swedish Security Technology Research and Innovation Programme disseminates new knowledge generated by the research, which is translated and developed into new skills, techniques and products. The target groups for the MSB Research include academia, government, municipalities, county councils and county boards, the public and students at universities and colleges. The MSB also cooperates with scientists to communicate the results from research projects, including popular science summaries and workshops for a range of audiences. The program supports projects that demonstrate effective technology, systems, products and activities that can be adapted for use in society. An emphasis has been placed on improving synergies between users, research providers and industry.

Case studies

H

Security Research Case studies

The tender specifications request that the contractor undertakes 5 case studies. The case studies have been produced as separate 'standalone' documents.

It was agreed with the Security Unit in Phase 1 that four thematic case studies and one horizontal case study focusing on SMEs will be undertaken. The following topics were agreed:

- 1) Maritime Surveillance
- 2) Aviation Security (including explosives detection)
- 3) Crisis management (including social aspects)
- 4) CBRNE (chemicals, biological, radiological nuclear and explosives)
- 5) SMEs and their participation in security research (horizontal)

There are of course other important areas in which the ESRP has made significant investment, such as critical infrastructure protection, protecting mass transit systems. However, the cases provided a useful opportunity to assess in detail the projects supported in a sample of themes. At ex-post evaluation stage, other areas of the programme could perhaps be analysed through a case study approach.

Standardisation

I. Standardisation

An area of interest in both PASR and FP7 SEC is the scope for EU Security Research to promote investment in the development of standards. Through PASR, there was scope for supporting the development of pre-standards. A number of PASR projects supported, such as **STABORSEC (Standards for Border Security Enhancement)** and **SECONND** in the area of secure shipping containers, involved mapping out existing standards, and research to examine the feasibility of developing common minimum standards in particular areas (pre-standards).

STABORSEC provides a good example of a project supported through PASR that made positive achievements in mapping out technical standards, with evidence of follow-up standardisation activities being supported building on the work of this project in FP7 SEC.

Promoting Standards through European Security Research

PASR project example: STABORSEC

The enhancement of European border security level requires the strengthened interoperability of technologies deployed at borders. STABORSEC was a supporting activity (prelude to CSAs under FP7) and among the activities carried out were the identification of technical standards in this area. The project was designed to build on the research results produced by the border security group of the European Security Research Advisory Board, and other European research projects. STABORSEC helped to identify standards and the way in which they are assessed, including evaluation mechanisms for testing conformity.

The STABORSEC project delivered value by producing a detailed inventory of standardisation efforts to date, and of possible future standards that might be used to promote greater interoperability in land border security. The project provides a useful illustration of a project in which the research results have been used. **STABORSEC** is being followed up both through general European standardisation activities (a mapping exercise to identify standards across different areas of security research), and through follow-up projects on standards in FP7, notably Effisec, which also focuses on border security and

A number of projects have been supported that related to standards across different thematic areas. This includes **EFFISEC** (land border control), **ESCORTS** (SCADA Supervisory Control and Data Acquisition) **CREATIF** (CBRN). Some of the projects supported in FP7 SEC build directly on the progress achieved during PASR. For example, STABORSEC was viewed as one of the direct forerunners to CREATIF.

Promoting Standards through European Security Research - FP7 SEC project example: CREATIF

CBRNE testing and certification - a networking strategy to strengthen cooperation and knowledge exchange

Standardisation is a significant issue in the CBRN field. The absence of a common testing and certification process within the EU often limits the range of security products available to end-users. To address this situation, the CREATIF project set up a network of testing facilities for security-related products and services focused on CBRNE detection. Testing facilities involved in the network publish information about their expertise and testing capabilities / facilities in a database on testing facilities within EU27.

The network also provides a forum for policy makers, CBRN end-users and other stakeholders, including industry and the European Committee for Standardisation (CEN) to work together on standardisation. An advisory board of users and industrial experts has been set up and has a specific role in some project deliverables. Users have also been invited to attend workshops on particular topics. Users, in this case private testing facilities, stand to benefit commercially should a more open certification and labelling regime with improved mutual recognition of testing procedures and common minimum requirements within the EU.

Standardisation

According to the **discussions with CEN-CENELEC** as part of the evaluation to assess progress in respect of standards through ESRP, a number of points were raised in relation to standards. First, certain levels of maturity in particular areas of security research are first needed in order to be able to develop standards, secondly, there needs to be strong consensus among industry stakeholders in order to .

In the wider security area (outside the 7th RTD Framework Programme) to date, relatively poor progress has been achieved in the standardisation area. However, some developments have been achieved, for example, in the area of high-tech ICT, GSM (security encryption), etc. Security-related areas in which there has been progress to date includes: a Standard for management of security systems (ICT-related), work on emergency services, Security and safety of bio-security laboratories, Personal protective equipment (formal Directive on equipment in industrial use, and there has been progress in respect of CBRN equipment) and informal standardisation or workshops.

With regard to **formal standardisation activities**, the European standards organisations have been asked to undertake a mapping exercise of existing standards with a view to the possible issuing of a European Standards Mandate in the area of security. However, the activities to date are relatively limited and outside the scope of this evaluation. Nevertheless, it is worth highlighting some of the committees that have been set up that are of relevance to FP7 Security Research and may be addressed in future calls.

Table 1: Standardisation activities

- Committee on personal identification – signatures and cards (request from Commission to upgrade workshop agreement into formal standards)
- Committee on biometrics
- Committee on RFID (radio frequency identification) – security aspects
- Supply chain security – however, no activities to date
- Airport and aviation security – currently only dealing with the qualification of personnel (background checks on security personnel, non-technical aspects)
- Horizontal committee – societal and ethical committee.
- Aviation security – strong consensus from industry, national governments and regulatory authorities
- Meeting on body scanners – no technical issues requiring a standard, code of conduct for operatives using body scanners was discussed but DG MOVE

Among the various committees identified above, it was felt that the societal and ethical committee could become increasingly important in future, since it relates very directly to the security research agenda. The European Commission's preference is to make the transition from a bottom-up to a top-down approach to the development of standards (since many standards are industry and regulatory authority driven, but this can take a very long period of time to come to fruition).

DG ENTR recently issued a **Mandate to the European standards organisations** to undertake a mapping exercise to identify scope for standards in particular areas of security. There is interest in developing a better understanding of the baseline situation across different areas of standards. However, an issue raised by the ESOs was the difficulty in identifying appropriate expertise for technical standards.

The lead times involved in financing European standards are quite long. CEN-CENELEC can take part in research projects. However, since these are EU financed, they receive no actual funding. Grant financing can take up to a year to organise. There could however be some advantages to a top-down approach,

Standardisation

such as getting key stakeholders around the table, giving some publicity to areas of standardisation where the EU has potential to provide an appropriate impetus.

A number of **informal standardisation activities** have also been identified in the security research area.

- Impact-related vehicle security barriers (anti-terrorist barriers). The workshop was driven by the security services in the UK, and focused on improving the technical performance of barriers,
- Secure containers – two calls, one under PASR and the other FP7 SEC have focused on Secure containers and some preliminary scoping of possible standards has been undertaken
- Galileo – services for tracing or tracking dangerous good transport

A challenge in achieving further progress is the need for extensive coordination and cooperation between different Commission DGs. Cooperation is required, for example, with DG MOVE in the field of aviation security, DG MARE (Maritime Security) and with DG JLS and FRONTEX on border security.

In conclusion, there are evidently interesting possibilities in the standards area, however, in practice, it is too early to provide a full assessment of progress.

Future perspectives

J

Future perspectives

Overview

Examples of relevant developments since the intervention logic was drawn up are summarised in the following table. These need to be taken into account in terms of planning for FP8:

EU Security Research – future perspectives

Evolution of primary legislation – the adoption of the Lisbon Treaty and its coming into force in December 2009 strengthened the legal base for coordination at EU level on internal security (while respecting subsidiarity principles). For example, there was the strengthened security dimension in respect of external actions.

Security-specific regulatory developments – for example, in the field of aviation security, in 2008, common basic standards on civil aviation security were drawn up in Regulation (EC) No 300/2008 supplemented by detailed implementing rules in April 2009 (Commission Regulation (EC) No 272/2009)

The ESRI report and establishment of an EU Security Research and Innovation Agenda – the ESRI report provides a strategic framework for security research. Since the exercise was stakeholder-driven, this can be seen as an important development shaping the strategic direction and content of the annual work programmes.

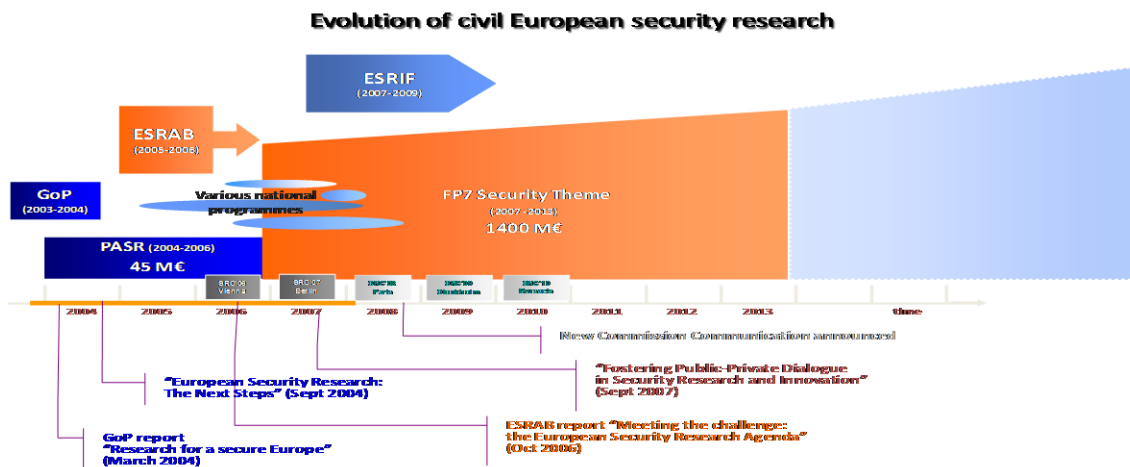
Policy developments – since FP7 was adopted developments include a 2010 Communication in the field of aviation security on security scanners, the adoption of the EU CBRN Action Plan in 2009, a policy package from 2006 on the European Programme for Critical Infrastructure Protection (EPCIP) and a policy Communication in 2008 on Reinforcing the Union's Disaster Response Capacity.

Security and crisis incidents – incidents that have occurred since the FP7 Security Research programme was adopted affect the overall security environment, and the need to update and keep close track of new and emerging threats. For example, in the area of crisis management, the Haiti earthquake showed the need for a coordinated EU rapid response.

Societal debate in response to security incidents and emerging security threats – EU Security Research and the activities supported in annual calls are influenced by concerns for the ethical and societal aspects. There has been intense debate on issues around data protection in some areas of security such as aviation and issues around privacy and ethics in respect of body scanners, surveillance and the detection of ‘abnormal’ behaviour.

The various developments in EU security research – regulatory, policy, societal and incident-based - influence the overarching framework in which FP7 Security Research interventions are implemented. The main developments are summarised in the following Figure:

Figure 1: Evolution of civil European security research



Future perspectives

J

Source: DG ENTR's Security Unit, H3

EU Security policy and the Lisbon Treaty

It is important to note in planning for FP8, that the legal base has evolved since the FP7 Programme Decision. In particular, a key development was the ratification of the Lisbon Treaty and its entry into force in December 2009. This allows strengthened scope for the EU's Security Research programme to support additional activities, and potential synergies for example in the area of EU external actions.

There are various areas of the Treaties relating to external EU security matters. Title V of the Consolidated Treaty on European Union (TEU) sets out General Provisions on the EU's External Action (Chapter 1) and Specific Provisions on the Common Foreign and Security Policy (CFSP) (Chapter 2, Section 1) and the Common Security and Defence Policy (ESDP) (Chapter 2, Section 2). In addition, Part Five of the Treaty of the Functioning of the European Union (TFEU) refers to External Action by the Union. Article 42 TEU states that the main objective of the ESDP is to provide the Union with operational capacity drawing on civil and military assets. 'The Union may use them on missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter. The performance of these tasks shall be undertaken using capabilities provided by the Member States.

Article 43(1) TEU is also relevant. 'The tasks referred to in Article 42(1), in the course of which the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including supporting third countries in combating terrorism in their territories.

In respect of humanitarian aid, Article 214 (1) TFEU states that 'the Union's operations in the field of humanitarian aid shall be conducted within the framework of the principles and objectives of the external action of the Union. Such operations shall be intended to provide ad hoc assistance and relief and protection for people in third countries who are victims of natural or man-made disasters, in order to meet the humanitarian needs resulting from these different situations'. The ESRIF report points out that humanitarian crises are a major concern for all actors in the EU's external Crisis Management system. 'The EU has a number of Community instruments specifically designed for addressing crisis situations, and operates usually in cooperation with international actors, its Member States and local organisations'.

Article 222 TFEU introduces a Solidarity Clause in the event of a terrorist attack or a natural or man-made disaster. Article 222(1) states that the Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to: (a) - prevent the terrorist threat in the territory of the Member States; protect democratic institutions and the civilian population from any terrorist attack; assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack; and assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

Article 176 TFEU focuses on energy security; it states that 'in the context of the establishment and functioning of the internal market and with regard for the need to preserve and improve the environment, Union policy on energy shall aim, in a spirit of solidarity between Member States, to

Future perspectives

J

[.....]....(b) ensure **security of energy supply in the Union**. While an important area, it should be pointed out that energy security is mainly the remit of DG Energy and that energy-related projects are not funded through FP7 Security Research.

Article 196 TFEU on Civil protection refers to the importance of improving the effectiveness of systems for preventing and protecting against natural or man-made disasters. In particular, clause 1 (Art. 196(1)) states that ‘the Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters’. Union action shall aim to: (a) support and complement Member States' action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union; (b) promote swift, effective operational cooperation within the Union between national civil-protection services; and (c) promote consistency in international civil-protection work.

In the table below, a summary overview is provided of the various areas of competence as set out in the Treaty on European Union (TEU) and the Treaty of the Functioning of the European Union (TFEU). The types of interventions funded through FP7 that are relevant in contributing to these areas are indicated.

Table 2: Overview of legislative provisions in Lisbon Treaty of relevance to FP7 Security Research

<i>Title in Lisbon Treaty</i>	<i>Description</i>	<i>Article</i>	<i>Policy areas</i>	<i>Types of interventions that could be funded in FP8 Security Research*</i>
Title V TEU	Provisions on the Union's External Action Service and specific provisions on the Common Foreign and Security Policy	Article 21 - 46 TEU	External Action, CFSP	Dissemination and networking events that promote coordination
Title III TFEU	Cooperation with Third Countries and Humanitarian Aid	Article 208 – 214 TFEU	Development, Cooperation, Humanitarian Aid	Crisis Management
Title VII TFEU	Solidarity clause	Article 222 TFEU	Solidarity Clause	Joint cooperation projects between Member States' authorities on the field of terrorism and in respect of strategies and approaches for responding to internal EU natural or man-made disasters. Opportunities for institutional bridge-building and whole-of-society capability development
Title XXI TFEU	Energy	Article 194 TFEU	Energy security (security of energy supply)	Scope for discussing with DG Energy possible research activities within FP8 SEC?
Title XIX TFEU	Research and technological development and space	Articles 179 - 190 TFEU	Research and technological development and space	Underpins all RTD activities including those of EU Security Research
Title XXII TFEU	Civil protection	Article 196 TFEU	Civil protection - improving the effectiveness of systems for preventing and protecting against natural or man-made disasters.	Crisis management and emergency response projects Situation awareness projects

Future perspectives

J

While FP7 Security is a civilian research programme, there are **areas of research interest that are common to both civil security within the EU and external actions such as crisis management and humanitarian aid / relief**. This suggests a need for closer cooperation in order to maximise synergies, better exploit potential and to avoid duplication of research efforts. This could be achieved through the framework of the existing Framework Cooperation Mechanism with the EDA.

ESRIF and non-legislative evolutions

The work of ESRIF, which ran in parallel with the early stages of the implementation of FP7 SEC, involved a systematic analysis of civil security-related capability needs and a Security Research Programme has been implemented following the successful implementation of the PASR Preparatory Action. The Decision establishing the programme¹⁰ recognises however the need to ensure that where areas of 'dual-use' technology, *'close coordination with the activities of the European Defence Agency will be needed in order to ensure complementarity'*.

ESRIF¹¹ - the European Security Research and Innovation Forum (ESRIF) was set up in 2007 and involved two years of work, with more than 600 experts and 65 personalities from all over Europe. The experts were engaged in a debate in an open forum about aspects of European Research and Innovation considered essential to enhancing the security of EU citizens. The main objective of ESRIF was to develop a medium-long term strategy for EU Security Research in the form of a European Research and Innovation Agenda. The work of the group placed a strong emphasis on dialogue between public and private stakeholders in the research community. Other key aims were to share ideas, views and best practices in order to make better use of existing capabilities and to enhance the use of technology in security-related domains.

The process involved different types of stakeholders: policy makers, representatives from industry and end-users of security research, academic and research institutions. A series of working groups were set up focusing on different aspects of EU security research, such as crisis management, Foresight and Scenarios, CBRN, Border Security, Situational Awareness, the Security of Citizens and the Security of Critical Infrastructure. The ESRIF final report¹² was published in December 2009.

ESRIF underlined the need for an **anticipative or foresight approach to identifying and addressing evolving security threats**. A key conclusion was that R&D in the security field needs to focus on strengthening Europe's resilience to threats and its ability to efficiently recover from crises. This includes also enhancing the cohesiveness and robustness of societal systems and their interface with technologies. Other key suggestions include the need for a **more systematic approach to capability development** to address the increasing complexity of security and the emergence of new and unforeseen threats. Another key recommendation is the need for a more systemic approach to security in line with the concept of **security by design**.

¹⁰ DECISION No 1982/2006/EC

¹¹ More information on ESRIF is available on the ESRIF website: www.esrif.eu

¹² ESRIF Final report from the European Security Research and Innovation Forum - European Security Research and Innovation in support of European Security policies (December 2009)

Future perspectives

J

In response to the work of ESRIF, the Commission issued a Communication on 21 December 2009¹³ - *A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations*. The Communication recognises the **evolving nature of security threats** faced by the EU. *'The fight against terrorism and organised crime, the protection of the external European borders and civil crisis management have gained importance in our daily life. Climate change, if not properly addressed, could lead to major destabilising effects at global scale. At the same time, internal and external security are increasingly inseparable'*.

Looking ahead to the **preparation of FP8** and the evolving policy environment in respect of the implementation of the remainder of FP7 Security Research, the **EU2020 strategy** provides a strategic policy framework with various relevant references to R&D and innovation, as well as to particular policies relevant to security research. The strategy notes the challenges in *completing the European Research Area*, and refers to the need to develop a strategic research agenda focused on challenges such as energy security.

¹³ Commission Communication, of 21 December 2009 - A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations