Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration.

Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration

Final Report

Written by Technopolis Group
September 2015

technopolis |group|

EUROPEAN COMMISSION

Directorate-General for Migration and Home Affairs
Directorate B — Migration and Mobility
Unit B.4 — Innovation and Industry for Security

Contact: Gerburg LARSEN

E-mail: HOME-NOTIFICATIONS-B4@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration

Final Report

Directorate-General for Migration and Home Affairs
Directorate B Migration and Mobility / FP7 Security Research Actions

2015

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2015

ISBN 978-92-79-40838-0
doi:10.2769/46344

Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration

Final Report

Authors:

- Paul Simmonds, Technopolis Group
- Thomas Teichler, Technopolis Group
- Neil Brown, Technopolis Group
- Johanna Enberg, Technopolis Group
- Anders Hakansson, Technopolis Group
- Olivier Mallet, Technopolis Group
- Peter Stern, Technopolis Group
- Anna Karin Swenning, Technopolis Group
- Léonor Rivoire, Technopolis Group
- Jillian Yeow, Manchester Institute of Innovation Research (MIoIR)
- Deborah Cox, Manchester Institute of Innovation Research (MIoIR)
- John Rigby, Manchester Institute of Innovation Research (MIoIR)
- Simone Plances, VVA
- Pierre Hausemer, VVA
- Marco Bolchi, VVA
- Julia Rzepecka, VVA
- Julia Culver, Nomisma

Date: September 2015

Table of Contents

1. Introduction 1
1.1 This report 1
1.2 Key parameters of the evaluation 1
1.3 Structure of the Report 2
2. Methodology 3
2.1 Overall approach 3
2.2 Desk research 4
2.3 Analysis of statistical data 4
2.4 Participant survey 5
2.5 End-user survey 7
2.6 Stakeholder interviews 7
2.7 Case studies 8
2.8 Stakeholder workshop 9
3. Evaluation results 10
3.1 Overview of FP7 Security Research Actions 10
3.2 Evidence Building Block 1: Rationale (“why”) 19
3.3 Evidence Building Block 2: Implementation (“how”) 31
3.4 Evidence Building Block 3: Direct Achievements (“what”) 41
3.5 Evidence Building Block 4: Wider Achievements (“what”) 52
3.6 Evidence Building Block 5: European Added Value 63
3.7 Evidence Building Block 6: Conclusions on FP7 & outlook for H2020 70
4. Conclusions and recommendations 73
4.1 Conclusions 73
4.2 Recommendations 78

Table of Contents - Appendices

Appendix A Evaluation questions (EQs) 82
Appendix B Tabulation of evaluation questions and EBBs 83
Appendix C Typology of end-users 84
Appendix D Organisational affiliations of interviewed stakeholders 85
Appendix E Case study executive summaries 87
Appendix F Case studies on security research 109
F.1 Ethics in security research 110
F.2 Forms of end-user involvement in projects 118
F.3 Shaping the end-user landscape in the EU 126
F.4 Analysis of the complementarity of CBRNE security research in FP7 and projects involving EDA 133
F.5 Impact on the competitiveness of the European security industry 139
F.6 Productive Use of IPR from Security Research Actions 146
F.7 Demonstration projects 153
F.8 Protecting critical infrastructures – Port Security 164
F.9 Tools, methods and resources to restore safety and security in case of crisis 173
F.10 The involvement of the citizen in security research 179
F.11 Project clusters – success factors for cross-project collaboration 190
F.12 Participation of smaller EU countries in FP7 Security Research Actions 197
F.13 Dealing with challenges in diverse project settings involving numerous types of partners 211
F.14 The significance of standardisation for Security Research Actions 218
F.15 The influence of FP7 SRAs on national research programmes 223
Appendix G Summary of the stakeholder workshop 231
Appendix H Intervention logic 235

List of Tables

Table 1: Tabulation of evaluation dimensions and data / information collection methods 4
Table 2: Distribution of participations by organisation type....6
Table 3: Distribution of projects and participations by mission area 6
Table 4: Sample of stakeholder interviews 8
Table 5: List of case studies 9
Table 6: Distribution of projects, participations and funding by mission 15
Table 7: Share of different actors in Security Research mission participations 16
Table 8: Mission areas with highest/lowest participation rates of different actors 16
Table 9: Share of Security Research projects and participations by instrument.... 17
Table 10: Share of participations in each instrument by type of actor.... 17
Table 11: Share of EC contributions by different types of actors 17
Table 12: Participations by different actors – Security vs. Cooperation Programme ... 18
Table 13: Share of unique organisations participating in single or multiple projects... 18
Table 14: Distribution of proposals submitted and EC contribution requested by call 20
Table 15: Demand for Security Research and the FP7 Cooperation Programme.... 21
Table 16: Security Research participations, by mission and type of actor 21
Table 17: Are the objectives of the FP7 Security Research Programme relevant to the needs of different EU stakeholders? (n = 708)....22
Table 18: Are the mission areas of the FP7 Security Research Programme relevant to the needs of different EU stakeholders? (n = 708) 23
Table 19: Overview of FP Security Research, by Work Programme (WP), Instrument and Mission 27
Table 20: Distribution of projects, participations and funding by mission.... 28
Table 21: Time to grant statistics for FP7 Security Research Actions in days 33
Table 22: Projects producing publications (n=61) 42
Table 23: Number of publications per project for key comparators 43
Table 24: Projects, participations and EC contributions, by country 44
Table 25: Geographical participations per million population....45
Table 26: Major participants in the Cooperation Programme (not SEC) 46
Table 27: Gender distribution of key project personnel 46
Table 28: Share of workforce that is male 46
Table 29: Top peer-reviewed journals, sorted by number of Security Research publications 56
Table 30: Top peer-reviewed journals, by journal rank indicator....56
Table 31: Security Research Publications, by journal subject area 57
Table 32: Total direct funding leveraged, per €1 of EC contribution.... 61
Table 33: Average EC contributions per project and participation, by mission area....63
Table 34: National civil security research programmes (selection) 69

Table 35: Tabulation of evaluation questions and EBBs 83
Table 36: Types of end-users addressed in the end-user survey 84
Table 37: Organisational affiliations of stakeholders who were interviewed 85
Table 38: List of case studies 87
Table 39: Topic areas mentioning "ethics" in the wording of calls 112
Table 40: Number of Ethics Reviews in the Security Research theme, per year and total 113
Table 41: Number of processed Security research projects where ethical issues were identified 113
Table 42: Projects funded under area 10.6.5: Ethics and justice 115
Table 43: FP7 Security projects coordinated by end-users 121
Table 44: FP7 Security Research projects reporting IPR 149
Table 45: IPR reporting across the FP7 Cooperation Specific Programme 149
Table 46: Calls for Phase I and II demonstration projects 155
Table 47: Distribution of demonstration projects by mission 155
Table 48: Distribution of demonstration projects by theme 155
Table 49: 'Typical' characteristics of Phase I and II demonstration projects 156
Table 50: Distribution of Phase I projects by theme 157
Table 51: Phase II projects by theme, and project objectives 159
Table 52: List of projects with the participation of port authority bodies 169
Table 53: Distribution of projects by mission 170
Table 54: FP7 Security Research Programme participation and funding, by MS 198
Table 55: Participations (and funding) relative to population size, top 5 countries 199
Table 56: Participations (and funding) relative to GDP, top 5 countries 199
Table 57: Participations (and funding) relative to researcher population, top 5 199
Table 58: Participation in the FP7 Security Research Programme and the Cooperation Specific Programme 200
Table 59: Luxembourg – measures of participation levels 201
Table 60: Luxembourg – EC contributions 201
Table 61: Slovakia – measures of participation levels 202
Table 62: Slovakia – EC contributions 203
Table 63: Latvia – measures of participation levels 205
Table 64: Latvia – EC contributions 205
Table 65: Estonia – measures of participation levels 206
Table 66: Estonia – EC contributions 206
Table 67: The main actors in FP7 Security Research 213
Table 68: Divergence issues across the project process 213
Table 69: Distribution of projects by mission 220
Table 70: Number of projects and governmental contributions to security research from 2006 -2013 (approximate values) 229

List of Figures

Figure 1: General evaluation framework....3

Figure 2: Participant survey – population and response rate....5

Figure 3: Overall structure of FP7 Security Research Programme....12

Figure 4: Which of the following elements were objectives of the project, and to what extent have they been achieved (or are likely to be achieved in the future)? (n = 599) 29

Figure 5: How satisfied or dissatisfied were you with the following aspects of the FP7 Security Research project cycle and its implementation? (n = 585)....34

Figure 6: Estimate the share of your / your organisation's overall project input that was spent on the following administrative tasks (participants) (n = 573)....36

Figure 7: Estimate the share of your / your organisation's overall project input that was spent on the following administrative tasks (coordinators) (n = 92)....37

Figure 8: How does the FP7 Security Programme compare with other similar research programmes in terms of weight of administrative requirements? The requirements of the FP7 Security Research Programme are... (n=461)....37

Figure 9: To what extent have the simplification measures that were introduced with the launch of FP7 resulted in improvements? (Participants) (n = 573)....39

Figure 10: To what extent have the simplification measures that were introduced with the launch of FP7 resulted in improvements? (coordinators) (n = 92)....39

Figure 11: Which of the following elements were objectives of the project, and to what extent have they been achieved (or are likely to be achieved)? (project coordinators) (n = 599)....48

Figure 12: Indicate whether any of the following have resulted (or are expected to result) from the FP7 projects (n = 611)....49

Figure 13: To what extent do you believe participation in the project had the following positive impacts on your organisations (n = 594)....50

Figure 14: What has been the impact of the FP7 Security Research Programme overall in relation to each of the following programme objectives? (n = 269)....52

Figure 15: What has been the impact of the programme overall in relation to European Security Industrial Policy and Industry Market? (n = 257)....53

Figure 16: Security research and standardisation....54

Figure 17: What has been the impact of the programme overall on the following? (n = 259)....58

Figure 18: Overall, how did the costs and benefits of participation in the FP7 Security Programme compare (n=506)?....59

Figure 19: Indicate the extent to which your project was effective in leveraging the research activities of other actors (n = 377)....61

Figure 20: To what extent do the following aspects of the FP7 Security Programme provide (European) added value? (n = 85)....64

Figure 21: What is likely to have happened in the absence of the support provided by the FP7 Security Programme? (n = 401)....65

Figure 22: Could your project(s) have been supported by an existing national or international funding scheme? (n =362)....66

Figure 23: If 'No' (your project could not have been supported by another scheme), why not ...? (n = 293)....67

Figure 24: To what extent do you believe that the €1.4b FP7 Security Research budget was sufficient to achieve its stated objectives? (n = 87) 67

Figure 25: To what extent do you agree with each of the following statements as justification for the continuing need for EU funding of Security Research? Continued EU funding for Security Research is required because… (n = 570) 71

Figure 26: The evaluation questions from the Technical Specifications 82

Figure 27: Example for mapping of FP7 Security Research projects 130

Figure 28: The multiple functions of ports..... 165

Figure 29: Distribution of projects with a "port security" dimension by mission.....168

Figure 30: European security research programme policy cycle 182

Figure 31: Flood event crisis field trial 184

Figure 32: Citizen summits as a mechanism for the involvement of citizens 185

Figure 33: Presentation of the DEMOSEC Cluster on the IRISS website.....191

Figure 34: Website of the joint final DEMOSEC conference..... 194

Figure 35: Project optimisation – an idealisation..... 216

Figure 36: Distribution of projects with a "standard" dimension by mission 219

Figure 37: Intervention logic.....235

List of Abbreviations

ANR	French National Research Agency
BCM	Business continuity management
BTWC	The Biological and Toxin Weapon Convention
CBRNE	Chemical, biological, radiological and nuclear (substances) and explosives
CCTV	Closed-circuit television
CDP	Capability Development Plan
CDTEG	European Customs Detection Technology Expert Group
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CNR	National Research Council (Italy)
CORDA	COmmon Research DAta warehouse
CoU	Community of Users
CP	Collaborative research project
CP-CSA	Combined collaborative project and coordination and support action
CP-FP	Collaborative small- or medium-scale focused research project
CP-IP	Large scale integrating project
CSA-CA	Coordination and support action – coordination action
CSA-SA	Coordination and support action – support action
CSDP	Common Security and Defence Policy
CSO	Civil society organization
CWC	Chemical Weapon Convention
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG ECHO	Directorate-General Humanitarian Aid and Civil Protection
DG ENER	Directorate-General for Energy
DG ENTR	Directorate General for Enterprise and Industry
DG ENV	Directorate-General for the Environment
DG GROW	Directorate-General Internal Market, Entrepreneurship, Industry and SME
DG HOME	Directorate-General Migration and Home Affairs
DG MARE	Directorate-General for Maritime Affairs and Fisheries
DG MOVE	Directorate-General Mobility and Transport
DG RTD	Directorate-General for Research and Innovation
DG SANTE	Directorate-General Health and Food Safety
DG TAXUD	Directorate-General for Taxation and Customs Union
DGA	Direction Générale de l'Armement (France)
DLR	German Aerospace Center
DPI	Deep packet inspection
EAB	Ethical Advisory Board
EAV	European added value
EBB	Evidence Building Block
EC	European Commission
EDA	European Defence Agency
EDEM	European Defence Equipment Market
EDTIB	European Defence Technological and Industrial Base
EEAS	European External Action Service
EFC	European Framework Cooperation

ENLETS	European Network of Law Enforcement Technology Services
EOS	European Organisation for Security
ERA	European Research Area
ERAC	European Research Area Committee
ERCC	Emergency Response Coordination Centre
ESA	European Space Agency
ESO	European Standards Organisations
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
ESS	Emergency Support Systems crisis management project
EU	European Union
EUCI	European Classified Information
EQ	Evaluation Question
FP	Framework Programme
GDP	Gross Domestic Product
GoP	Group of Personalities
HES[1]	Higher or Secondary Education Organisation
H2020	Horizon 2020
IAEA	International Atomic Energy Agency
ICT	Information and Communication Technology
IMO	International Maritime Organisation
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
ISPS	International Ship and Port facility Security
JIP CBRN	Joint Investment Programme for CBRNE
JTI	Joint Technology Initiative
KPI	Key performance indicator
LIBE	Civil Liberties, Justice and Home Affairs Committee of the European Parliament
MS	EU Member State
NCP	National Contact Point
NOE	Network of excellence
NPT	Nuclear Non-proliferation Treaty
OPCW	Organization for the Prohibition of Chemical Weapons
OTH[1]	Other (types of participant organisation)
PASR	Preparatory Action for Security Research
PCP	Pre-Commercial Procurements
PPE	Personal protective equipment
PPI	Public Procurement of Innovative solutions
PRC[1]	Private for Profit Organisation (excluding education)
PSC	Political and Security Committee
PUB[1]	Public Body (excluding research and education)
R&T	Research and technology
REA	Research Executive Agency

[1] The abbreviations for the organisation type of participants (i.e. HES, PRC, PUB, REC and OTH) are used in this report in line with the CORDA definitions.

REC[2]	Research Organisations
RTD	Research and Technological Development
RTO	Research and Technology Organization
SESAM	European Commission's project-monitoring system
SGDSN	General Secretariat for Defence and National Security (France)
SIA	Surveillance impact assessment
SJR	Scientific Journal Ranking
SME	Small and medium-sized enterprise
SOLAS	International Convention for the Safety of Life at Sea
SnT	Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
SRA	FP7 Security Research Actions
SRCA	Slovak Research and Development Agency
SSH	Socio-economic Sciences and Humanities
STSC	Security Technology Supply Chain
TBE	The Netherlands Institute for Applied Scientific Research
TNO	Theory-based evaluation
TRL	Technology reediness level
TTG	Time-to-grant
UITP	International Association of Public Transport
VTT	The Technical Research Centre of Finland
WIPO	World Intellectual Property Organisation
WP	Work Programme

[2] The abbreviations for the organisation type of participants (i.e. HES, PRC, PUB, REC and OTH) are used in this report in line with the CORDA definitions.

1. Introduction

1.1 This report

This report is the Final Report of the 'Final Evaluation of Security Research under the Seventh Framework Programme for Research, Technological Development and Demonstration (FP7)', which was commissioned, in 2014, by Directorate-General Enterprise and Industry (DG ENTR).[3]

A consortium led by Technopolis Group and including VVA, as well as the Manchester Institute of Innovation Research, conducted the research for this study in the period from August 2014 to August 2015. This report presents the detailed results and analyses, conclusions and recommendations from the evaluation. These are based on findings from data collection and analyses, drawing on desk research, data from the CORDA database, surveys of participants and end-users, stakeholder interviews, a series of case studies, and a stakeholder workshop.

This opening Section introduces the FP7 Security Research Programme and outlines the context, as well as the structure of the report.

1.2 Key parameters of the evaluation

1.2.1 Activity to be evaluated

The evaluation concerns the **Security Research Programme** of FP7. The FP7 Security Research Programme (henceforth also called Security Research Actions) represents one of the ten thematic areas of the FP7 Cooperation Specific Programme.

The security research activities under FP7 are of special **significance for two reasons**:

- The FP7 Security Research Programme was the first fully-fledged European security research programme, building on a series of European strategic and policy initiatives that were launched during the early 2000s and responding also to the events of 9/11;
- The FP7 Security Research Programme had a budget of around €1.4b (€1.26b EU contribution), which far exceeds the resources available to even the largest national security research programmes, which is not the case for other themes covered by FP7.[4]

Further background information on the programme, including an overview of its origins, objectives, scope, implementation and activities, is presented in Section 3.1.

1.2.2 Rationale for the evaluation

The rationale for the evaluation is set out in Article 7 of the Council Decision on FP7, which requires the Commission to carry out an external evaluation by independent experts of its rationale, implementation and achievement.

The final evaluation of FP7 security research will be used to both, assess the effectiveness of the FP7 Security Research Actions and provide recommendations for the implementation of the Secure Societies Challenge of Horizon 2020, the successor programme to FP7.

The results of this study constitute part of the evidence base for the overall FP7 Ex-post Evaluation.

[3] On 1 January 2015, the 'Policy and Research in Security' Unit moved from DG ENTR to DG HOME and became Unit HOME-B.4 Innovation and Industry for Security. At the same time, the name of DG Enterprise and Industry was changed to DG Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). In this report, the different designations are used according to context and timing.

[4] For example, France and Germany spent €15 million and €57 million per year on security research in the period between 2006/7 and 2013.

1.2.3 Scope of the evaluation

The evaluation covers all parts of the **FP7 Security Research Programme** across EU Member States and Associated States from the start of FP7 in 2007 through the time that the study is being conducted (notwithstanding that some relevant FP7 activities will continue at least until 2016).[5] In order to properly address all aspects of the evaluation objectives, the study assesses both programme-level performance issues and project-level results and impacts, where feasible.

1.2.4 Evaluation objectives

The overall objective of the evaluation was to "… evaluate the relevance, effectiveness, efficiency, coherence and EU added value of FP7 Security Research in relation to the relevant overarching political and operational objectives of FP7 in support of European Security industrial Policy and Europe 2020."

The evaluation was both **summative and formative**.[6] Specifically, the evaluation assessed the relevance, effectiveness, efficiency, coherence and EU added-value of the programme, with specific reference to the objectives of the various activities covered. This includes the potential use of the technologies produced by the projects as well as early evidence of (potential) impacts (in policy, knowledge and socio-economic contexts) and value for money.

1.2.5 Evaluation questions

Six standard dimensions (relevance, effectiveness, efficiency, EU added value, coherence and utility) were identified and addressed by **22 evaluation questions** (listed in Appendix A).

The findings were then grouped under Evidence Building Blocks (EBB) used by the European Commission for the FP7 Ex-post Evaluation and related thematic studies (see Appendix B).

1.3 Structure of the Report

The Report is structured as follows:

- Section 1 is the **Introduction** to the report;
- Section 2 details the methodological **approach**;
- Section 3 provides an overview of the FP7 Security Research Actions and presents the **findings** of the evaluation – structured according to the Evidence Building Blocks;
- Section 4 presents the **conclusions and recommendations** from the evaluation.

The report also contains several appendixes of supporting documentation and information, which are referenced in the main body of the report.

[5] FP7 calls for proposals started in 2007 and were published annually until 2013. Projects selected in the final (6th) call for proposals were expected to start in 2014 and should be concluded by 2016.

[6] A summative evaluation focuses on the outcome of a program, in contrast to a formative evaluation that assesses the development at a particular time.

2. Methodology

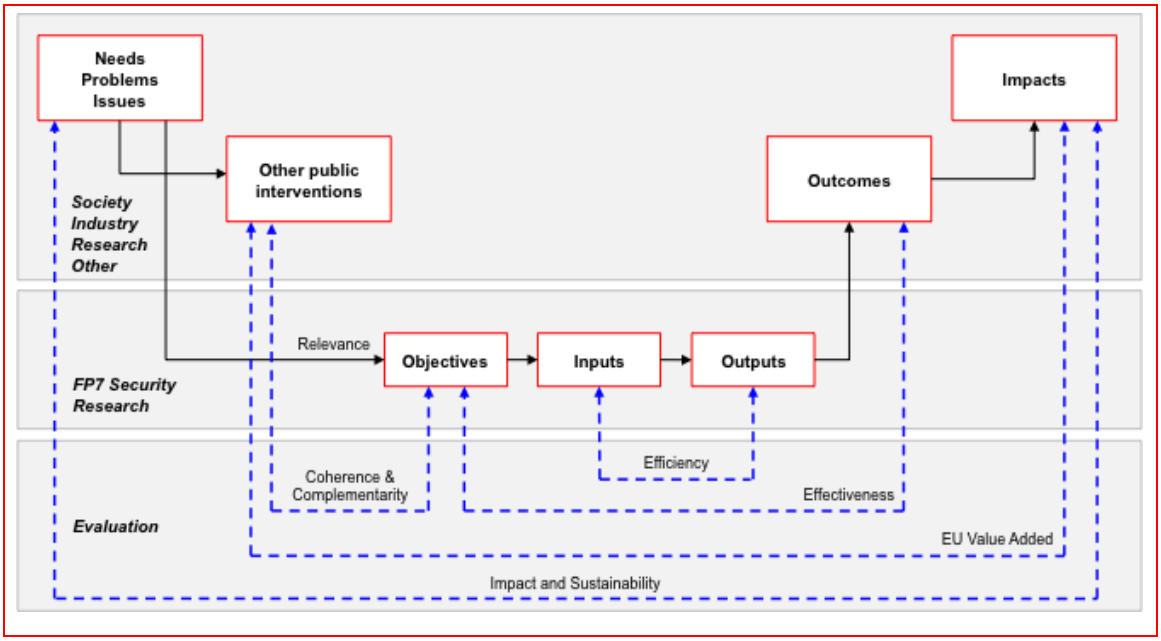
2.1 Overall approach

The overall approach used by the team followed current EU evaluation practice, and was based on a '**theory-based evaluation**' (TBE) framework that is especially suited to complex programmes like FP7, where other impact assessment methodologies (e.g. quasi-experimental methods) find it difficult to achieve satisfactory results.

The TBE framework is concerned with the programme theory and the assumptions of policy makers (and other stakeholders) about the preconditions, context and challenges that justified a particular policy intervention. Theory-based impact evaluations test assumptions (about problems and objectives) against the observed results, following different steps of the **intervention logic** from programme inputs to outputs to intermediate effects (outcomes) and ultimately to the wider effects (impacts). They explain why and how results have occurred and assess the contribution of the programme and of other factors to those achievements.

Figure 1 shows a generic framework that is commonly used in policy evaluation. It serves to explain how each of the six broad evaluation questions (e.g. relevance or efficiency) are linked to the specific intervention logic for the FP7 Security Research Programme.

Figure 1: General evaluation framework



Source: Technopolis

The project team used a **mixed-methods approach**, combining qualitative and quantitative methods in order to answer each of the evaluation questions, allowing a degree of simple triangulation, whereby multiple data streams and cross-tabulations provide a greater level of confidence in the correctness of the analysis, evaluation question by evaluation question. The evaluation made extensive use of each of the following methods:

1. Desk research, comprising documentary and statistical analyses;
2. Participant and end-user surveys;
3. Stakeholder interviews;
4. Case studies;
5. Focus group discussion (stakeholder workshop).

Table 1 presents a **schematic overview** of the contribution of each of the principal methods to each of the six overarching dimensions of the evaluation. This matrix is based on substantial past experience with FP evaluations, and captures the evaluation team's 'rules of thumb' whereby, for example, the semi-structured interviews with stakeholders were most helpful in understanding the political and industrial context and complementary initiatives, which were critical to testing relevance, EU added value and coherence. Stakeholders tended to have a less informed view of programme outcomes; as such, their views tend not to figure prominently in the consideration of programme impacts and value for money (effectiveness, efficiency). In contrast, the participant and end-user surveys produced useful feedback and statistics on all evaluation questions, even though respondents tended to have a better view of their own projects than the overall programme. These subjective data were used to gain an understanding of programme effectiveness as well as coherence, while capturing more qualitative insights on lessons learned and providing leads on potential impact case studies.

Table 1: Tabulation of evaluation dimensions and data / information collection methods

	Relevance	Effectiveness	Efficiency	EU Added Value	Coherence	Utility
Desk research	***	**	**	**	*	
Analysis of statistical data	***	***	***	***	***	***
Surveys (participants and end-users)	**	**	**	***	**	***
Stakeholder interviews	***	*	**	***	***	**
Case studies	**	***	*	**	*	
Focus Group (stakeholder) workshop	**	*	*	**	**	***

Source: Technopolis

In the following sub-sections, each of the data/information collection tools is presented in greater detail.

2.2 Desk research

Desk research and document review provided the basis for the collection of primary data. It helped the team to set up the analytical framework (programme logic and Key Performance Indicators (KPIs)), which shaped the design of the data collection tools. The desk research also allowed the team to begin to answer several of the evaluation questions. In particular, the issues of relevance, coherence and alignment were addressed directly through desk research. The desk research has also fed into the preparation of case studies, combined with case study interviews.

Specific findings from the desk research are presented alongside evidence from other sources in both Section 3.1 (background information on the Security Research Programme) and in the discussion of evaluation questions under each of the six EBBs (Section 3).

2.3 Analysis of statistical data

This study makes use of existing **statistical data provided by the EC CORDA** database, in particular:

- CORDA data (as of 20 June 2014), providing information on the 307 funded Security Research Programme projects included in the database, including budget, participant organisations etc;
- CORDA Research performance and impact reports data (as of 02 September 2014), a specific module of CORDA, providing information on outputs and achievements of finished projects. This module combines inputs coming from the project coordinators (inserted in the project final report) together with information from the assessment by Project Officers. As of 02 September 2014, final reports for 61 finished projects were recorded as having been processed. The analysis is based on these 61 projects, representing 20% of the entire FP7 Security Research portfolio, and hence focusing particularly on projects awarded early in the programme period (which tended to be the first to be completed).

The analysis of the CORDA data served several **purposes**: It was used as follows:

- To describe the statistics and patterns that have emerged over time in the implementation of the FP7 Security Research Programme as reported in the CORDA databases;
- To guide the selection and definition of evaluation indicators;
- To inform the plans for the desk research, survey questions and data analysis;
- To assess the usefulness of the contents for each of the evaluation questions.

The examination of CORDA data revealed that project, participation and proposal data all provide valuable background information and indicators for addressing many of the evaluation questions, and particularly those relating to relevance, effectiveness and efficiency. CORDA project reporting data (final report) more specifically offered the opportunity to analyse the achievements of a sub-set of projects across a number of different dimensions, therefore helping to address (mainly) questions of effectiveness. Further analysis served to complement the collection of qualitative data from interviews and surveys with quantitative information.

The results of the examination of the statistical data fed into the description of the Security Research Programme in the next Section and also the assessment of the evaluation questions in the subsequent Sections, where results are presented together with evidence from other sources.

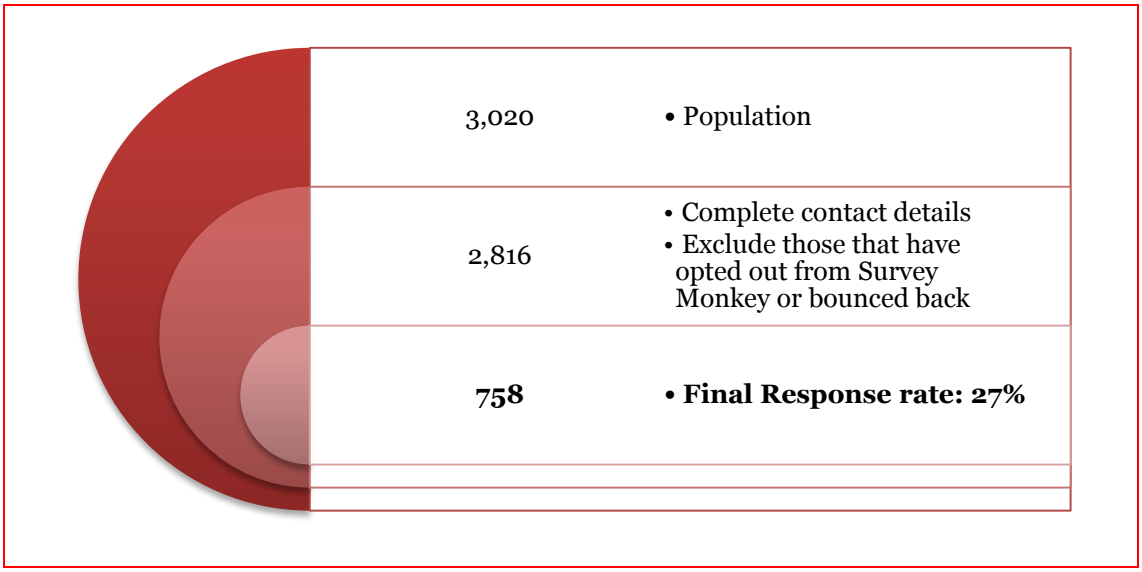
2.4 Participant survey

The project team designed and implemented **two online surveys** that were addressed to two key groups:

- A survey of all participants in FP7 Security Research Actions;
- A survey of wider end-users, which have not necessarily participated in FP7.

The survey of FP7 Security Research participants gathered feedback from beneficiaries on the majority of evaluation questions. It was launched on 6 November 2014 and concluded during the following month on 12 December 2014. The following figure illustrates the size of the overall population of participants compared with the number of participants that received the survey and those who responded to it.

Figure 2: Participant survey – population and response rate



Source: Technopolis

From the overall pool of 307 Security projects that had signed grant agreements by 20 June 2014, the team identified a **total population of 3,020** unique participant contacts, which were then contacted via e-mail and invited to participate in the survey.

From this population:

- 71 individuals (2%) had opted out from receiving these types of surveys, which in practice meant that they did not receive the request to participate; and
- 133 e-mails (4%) bounced back (i.e. the address was incorrectly recorded or was out of date), meaning these individuals did not receive the survey request either.

As such, a total of 2,816 participant contacts received the request to take part in the survey. All in all, 758 participant contacts responded. This corresponds to a response rate of 27% (of those receiving the survey), and represents a comparatively high response rate for an FP participant survey, particularly one of this length and complexity.

The sample is of a **good quality** in terms of its representation of the overall population:

- It includes participants from nearly all FP7 Security projects, with a response from *at least* one of the participating organisations in (287 out of 307). 93% of the projects supported;
- Altogether, the respondents had participated in FP7 Security projects 983 times, representing 26% of all participations;
- Furthermore, 86 of the respondents had been coordinators of at least one project, representing 30% of all project coordinators;
- The sample includes responses from 33% of all participating organisations (610 of 1,824).

The **sample distribution** by type of organisation also closely followed the distribution of the FP7 Security Programme overall (see Table 2).

Table 2: Distribution of participations by organisation type

	Participations	
Organisation type	**Population**	**Sample**
HES – Higher or Secondary Education Organisation	21%	24%
PRC – Private for Profit Organisation (excluding education)	43%	40%
PUB – Public Body (excluding research and education)	11%	11%
REC – Research Organisation	23%	23%
OTH – Other	3%	2%
Total	**3,741**	**983**

Source: Technopolis analysis of CORDA data, December 2014

Finally, the **structure** of the sample closely corresponds to that of the overall population. The following table compares the population and sample distribution of projects and participations across the mission areas of the programme. The differences between population and sample figures never exceed three percentage points.

Table 3: Distribution of projects and participations by mission area

	Projects			Participations	
Mission areas	**Population**	**Sample**		**Population**	**Sample**
Security of citizens	18%	20%		18%	17%
Security of infrastructures and utilities	17%	16%		19%	18%
Intelligent surveillance and border security	10%	10%		12%	11%
Restoring security and safety in case of crisis	18%	19%		20%	20%
Security systems integration, interconnectivity and interoperability	10%	9%		8%	7%
Security and society	15%	15%		13%	15%
Security Research coordination and structuring	11%	11%		11%	11%
(Other)	1%	0%		0%	0%
Total	**307**	**287**		**3,741**	**983**

Source: Technopolis analysis of CORDA data, December 2014

Not all respondents were asked (or answered) all questions, and so sample sizes vary between different sections of the survey results, as indicated in the tables and figures presented (i.e. n=x).

2.5 End-user survey

The end-user survey sought to obtain feedback from the **wider end-user community** about the relevance and impacts of the Security Research Programme overall, to corroborate and extend the view obtained from the participant survey. Moreover, the extent to which the capabilities of end-users have been improved as a result of the Security Research Actions is also a proxy for the improvement of the security of citizens.

The team developed a simple **typology** of end-users, which was used to identify and group end-users, also with the intention to identify patterns in their responses to the end-user survey. The typology of end-users is presented in Appendix C.

End-users were **approached in three different ways**:

- End-users constitute a sizeable part of the total population of FP7 Security Research beneficiaries, and were therefore addressed directly by the participant survey (discussed above). Indeed, over 200 of the responses received to this questionnaire came from those who self-identified their organisation as being an end-user of Security Research;

  Furthermore, the study team prepared and launched a survey specifically aimed at non-participating end-users. This survey went live on 6 November 2014, and remained open until the end of January 2015. The team sought to engage additional end-users in two ways;

- In the first instance, the project coordinators of all FP7 Security Research projects (283 individuals) were contacted and asked to send out invitations on behalf of the evaluation team, asking their respective end-user contacts, who were not project participants (e.g. members of advisory boards, workshop delegates, etc.), to respond to the online survey;

- In addition, National Contact Points (NCPs) were approached, introducing the evaluation and asking them to invite their end-user contacts to complete the online survey.

The **success of the approach was somewhat limited**. Only 27 end-users had responded by 5 January 2015, and many of these were from organisations that had participated in the FP7 Security Programme. Several options were discussed and it was agreed that those end-user organisations identified via the participant survey should be contacted again.

On 12 January 2015, the team **re-contacted 230 participating end-users** who had completed the participant survey and invited them to provide additional inputs. This resulted in 81 further responses from end-user participants, giving a total of 108 responses from end-users. Respondents came from 25 different countries and represented a range of different types of end-user organisations as follows:

- Public and private security services (21);
- Emergency services (19);
- Operators of / companies with critical infrastructure (11);
- Disaster relief and crisis management organisations (10);
- Policy-making organisations developing security-related regulation or strategies (10);
- Other (37).

The results of the end-user survey(s) are included within the findings section for each of the relevant evaluation questions under the six EBBs (Section 4). Again, responses to the questions were optional, so the number of responses received varies by question, and is indicated in the tables and figures recording the results of the surveys.

2.6 Stakeholder interviews

Overall the team carried out 100 interviews, of which 30 were conducted face-to-face. These stakeholder interviews **explored the evaluation questions in depth** in order to provide better insight and understanding of Security Research participation. Interviews also provided important input for subjects to be addressed in case studies.

Although interviewees were selected according to the type of stakeholder, there was an attempt to include stakeholders from a variety of participating countries. As a result, the team interviewed **stakeholders in a total of 20 countries**. These included:

- Thirteen EU countries receiving the largest or significant EC contributions to Security Research: Germany, the United Kingdom, France, Italy, Spain, the Netherlands, Sweden, Belgium, Austria, Greece, Poland, Finland and Denmark;
- Four selected EU countries for which the Programme is of relatively high importance compared to their overall participation in the FP:[7] Slovakia, Luxembourg, Estonia, and Latvia;
- Three Associated Countries with significant participation in Security Research: Israel, Serbia and Switzerland.

Appendix D lists the **organisational affiliations** of stakeholders who were interviewed for the purpose of this study, while Table 4 presents the number of interviews conducted for each stakeholder group.

Table 4: Sample of stakeholder interviews

Stakeholder group	No. of interviews
EU officials in DG Enterprise and Industry and other services (e.g. REA, DG MOVE, DG HOME, DG SANCO) and National Contact Points	10
Senior representatives with a security brief in relevant international and national administrations (e.g. German Ministry of Education and Research (BMBF), VDI, Swedish Defence Research Agency, UK Home Office, etc.)	9
Representatives from industry, including SMEs, and end-users (e.g. crisis management centres, police forces, civil security services, border guards, transport, etc.)	21
Representatives from relevant present and former high-level committees and advisory groups (e.g. ESRAB, ESRIF)	9
Senior members of major research groups from the public and private sectors (e.g. DLR, NLR, QinetiQ, VTT, etc.)	15
Other beneficiaries (demand and supply)	19
Other stakeholders, including international cooperation partners (e.g. ESA, EDA)	17
Totals	**100**

Source: Technopolis

In addition to the 100 stakeholder interviews, the team also conducted:

- A number of **background interviews** with Commission staff in DG ENTR (4); and
- Four or five interviews for each of the 15 **case studies** – all in all 70 interviews – with Commission staff, project participants and other stakeholders as part of the development of case studies (see next Section).

2.7 Case studies

A series of case studies was developed to showcase programme impacts and explore important issues. Given the complexity of the FP7 Security Research Programme, it was agreed that the case studies **should address horizontal issues** or topics. The final selection of case studies is listed in Table 5.

[7] As an indicator of the relative importance of the Security Research Actions for a country, a country's share of the Security Research Programme compared to its share of the Cooperation Programme measured in EC contributions and in number of participations was used.

Table 5: List of case studies

No.	Title
1	Ethics in security research
2	Forms of end-user involvement in projects
3	Shaping the end-user landscape in the EU
4	Analysis of the complementarity of Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) research in FP7 and projects involving the European Defence Agency (EDA)
5	The FP7 Security Research Actions' impact on competitiveness of European security industry
6	Productive use of IPR from Security Research Actions
7	Demonstration projects
8	Protecting critical infrastructures – Port security
9	Tools, methods and resources to restore safety and security in case of crisis
10	The involvement of the citizen in security research
11	Project clusters – success factors for cross-project collaboration
12	Participation of smaller EU countries in FP7 Security Research Actions
13	Dealing with challenges in diverse project setting involving numerous types of partner
14	The significance of standardisation for Security Research Actions (pilot case)
15	The influence of FP7 Security Research Actions on national research programmes

Source: Technopolis

The **data collection** process for the case studies combined primary and secondary research, starting with desk research to understand the origins of impact and the rationale / objectives / theory behind the actions and their achievements. The case studies also entailed interviews with between three and seven relevant interlocutors per case study (Commission staff, project participants and other stakeholders). In total, 70 interviews in the context of the case studies were undertaken.

Executive summaries of the 15 case studies can be found in Appendix E, while the full case studies are presented in Appendix F. The case studies have been used selectively to illustrate or further develop the evaluation findings set out in this report, and are typically presented in a separate text box within the relevant section.

2.8 Stakeholder workshop

A one-day focus group, i.e. a stakeholder workshop, was held on 29th April 2015, involving invited experts and the project team. The purpose of the event was to seek input from the assembled experts on the preliminary findings and conclusions of the evaluation (as presented in the first findings and recommendations report), and in particular with regard to the assessment of the relevance, efficiency, effectiveness and impact of the Security Programme. The intention was to also discuss possible ways in which to tackle challenges in the future, e.g. how to enhance the valorisation of projects, or how to strengthen end-user engagement. As such, individuals with a *programme*-level view of the FP7 Security Research Actions were invited to participate.

The workshop brought together 21 participants from 11 Member States and four European institutions. They represented national security authorities, research organisations and public funding bodies, as well as companies in the security sector (end-users). While approximately half of those participating had already contributed to the evaluation through participating in surveys or stakeholder interviews, the remainder were being consulted for the first time.

A summary of the discussion during the workshop is presented in Appendix G. The results from the workshop have also fed into the development of this Final Report.

3. Evaluation results

This Section presents the results of the evaluation. It is **structured according to the Evidence Building Blocks (EBBs)** and contains an introductory section about the FP7 Security Research Programme. While some part of this information will be replicated in later sections of this Section it is deemed useful providing contextual information and the basis for understanding the results presented under the different EBBs.

The six **evidence building blocks** (EBB) are:

- Evidence Building Block 1: Rationale ("why");
- Evidence Building Block 2: Implementation ("how");
- Evidence Building Block 3: Direct Achievements ("what");
- Evidence Building Block 4: Wider Achievements ("what");
- Evidence Building Block 5: European Added Value;
- Evidence Building Block 6: Conclusions on FP7 and outlook for H2020.

The **22 evaluation questions** were grouped under the different EBBs (in the case of EQ1 and EQ7 appearing under more than one EBB) as shown in Appendix B. Based on the intervention logic (Appendix H), indicators were developed as a means by which to test the programme's achievements on the different evaluation questions.

In the EBB sections below, **each evaluation question** is presented with corresponding key indicators before the evidence is set out. The analysis will bring together the evidence from the different stands of data collection, i.e. desk research, statistical data analyses, the participant and end-user surveys, and the stakeholder interviews. The structure of the presentation will vary according to the subject matter and due to the fact that not all questions will be addressed by evidence from all data sources.

3.1 Overview of FP7 Security Research Actions

3.1.1 Background to the FP7 Security Research Actions

The EU's multi-annual Framework Programme for Research and Technological Development is the main instrument for funding research and for realising the aims of the European Research Area (ERA). Its Seventh Framework Programme (FP7, 2007-13) included a €1.4b Security Research Programme, as one of ten themes within the Cooperation specific programme. This represented the **first, fully-fledged EU security research programme**, building on a series of European strategic and policy initiatives that were launched during the early 2000s and responding also to the events of 9/11.

The European Council adopted Europe's first **security strategy**, "A Secure Europe in a Better World," in December 2003, providing the basis for a new European security policy, including a framework for European security-related research in an enlarged Europe. The strategy outlined the global challenges and key threats. As a complement to the new security strategy, in 2004 the Council of Ministers (the General Affairs Council) decided to create an Agency in the field of defence capabilities development, research, acquisition and armaments.

In response to the 2003 strategy, the Commission established a **Group of Personalities** (GoP) to help identify principles and guidelines for a European Security Research Programme. Their report, '*Research for a Secure Europe*' (2004), advocates a comprehensive European approach to address security-related needs inside as well as outside EU borders, and argues, amongst other things, that a Secure Europe demands we do more to exploit our technological advantages through increased EU funding of R&D, improved coordination among national and European activities and the creation of new synergies between different research sectors.

As a follow-up to this report, the Commission adopted the **Communication** 'Security Research: The next Steps'[8], which subscribed to the main thrust of the GoP recommendations. One of the actions announced was the Commission's intention to create a '**European Security Research Advisory Board' (ESRAB**) in order to help define the focus of a new security research programme. The Board included high-level experts from a spectrum of stakeholder groups, including public and private users, industry, the European Defence Agency and research establishments. ESRAB published its report, '*Meeting the Challenge: the European Security Research Agenda*' in 2006, ultimately leading to the FP7 Security Theme targeting four security missions of high political relevance and relating to specific security threats.[9]

In parallel to the work of the high-level group, the Commission launched its **Preparatory Action in the field of Security Research** (PASR, 2003), which tested the rationale and objectives for *Community* action and laid the foundations for the launch of a European Security Research Programme within FP7. Between 2004 and 2006 an overall budget of €45m supported 23 collaborative projects mainly in the areas of access control, border control, transport, ICT and surveillance systems and - to a lesser extent - in the fields of critical infrastructure and Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) protection.

3.1.2 Programme objectives

The 7th Framework Programme overall pursued the general objectives described in Article 163 of the Treaty: to strengthen industrial competitiveness and to meet the research needs of other Community policies, thereby contributing to the creation of a knowledge-based society, building of a European Research Area and complementing activities at a national and regional level.

It sought to promote excellence in scientific and technological research, development and demonstration through four programmes: Cooperation; Ideas; People; and Capacities.

The **FP7 Cooperation Specific Programme** provided support for transnational cooperation in a number of thematic areas corresponding to major fields of knowledge and technology, including civil security, where the highest quality research is pursued to address various European socio-economic challenges. The main effort was directed towards improving industrial competitiveness, with a research agenda reflecting the needs of users across Europe.

The Council Decision concerning FP7 defined the objectives specifically for the **Security theme**, as follows:

> *To develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to stimulate the cooperation of providers and users for civil security solutions, improving the competitiveness of the European security industry and delivering mission-oriented research results to reduce security gaps.*[10]

In the Council Decision, security-related research was considered a fundamental building block for achieving a high level of security within the area of freedom, security and justice. It was designed to contribute to the development of technologies and capabilities, also in support of other Community policies in areas such as transport, civil protection, energy, environment and health.

---

[8] COM(2004) 590 final.

[9] ESRAB also recommended building up the necessary capabilities (ESRAB identified 120 capabilities) for safeguarding security in these mission areas and recommended the creation of a European Security Research and Innovation Forum (ESRIF) to foster greater dialogue (pan-EU consultation) and a shared view of European security needs in a longer-term perspective (20 years). The ESRIF report was published in 2009 and followed by a Communication from the Commission that was entitled, "A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations."

[10] Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-13).

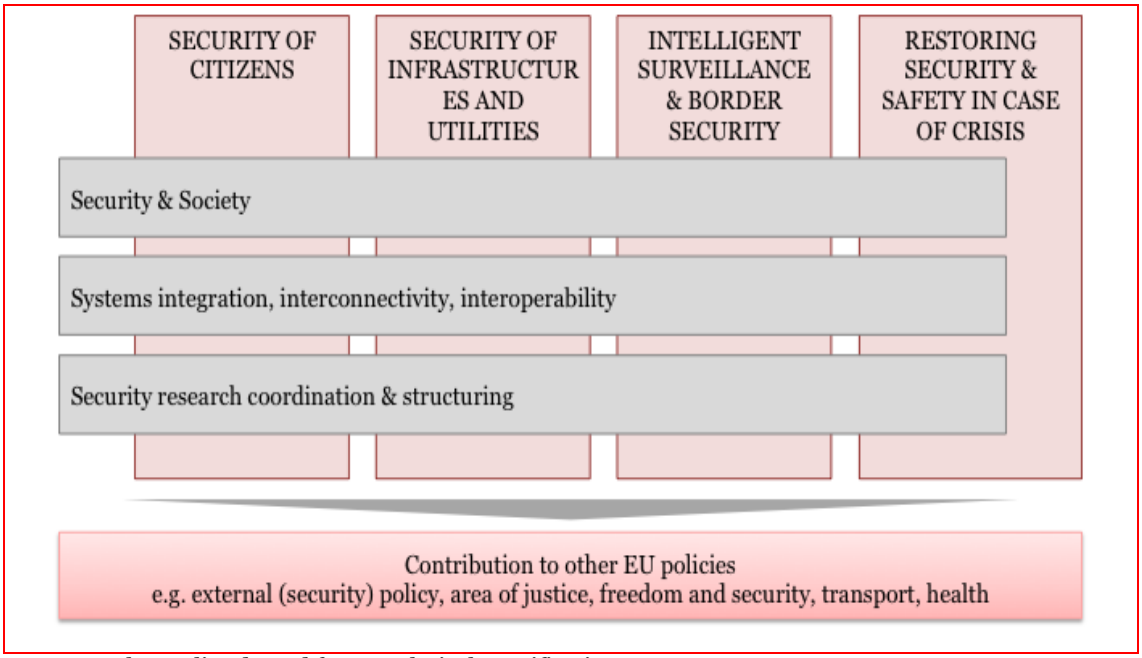
Existing security-related research activities across the EU suffered from a lack of coordination, critical mass of scale and scope, connections and interoperability. The Security theme therefore aimed at improving the coherence of the various national efforts in the Security context, in particular by developing a series of institutional arrangements to better focus the activities in this sector and promoting cooperation among the national and international actors, such as to avoid unnecessary duplication and to explore synergies wherever possible.

More detailed topic-level objectives were defined in the FP7 Security Research Work Programmes.

3.1.3 Scope and focus of the Programme

The Security theme of FP7 has an **exclusively civil application** orientation. Following the recommendations of ESRAB and the experience of the Preparatory Action, it was conceived as a mission-driven programme, addressing four main security missions and three domains of cross-cutting interest (see Figure 3). These missions were designed to ensure an appropriate level of political engagement, as well as improve the effectiveness and efficiency of more classic, technology-related research.

Figure 3: Overall structure of FP7 Security Research Programme



Source: Technopolis adapted from Technical Specifications

The four **mission areas** of the Security Programme are:

- Security of citizens: delivering technology solutions for civil protection, including bio-security and protection against risks arising from crime and terrorist attacks;
- Security of infrastructures and utilities: analysing and securing existing and future public and private critical/networked infrastructure (e.g. in transport, energy, ICT), systems and services (including financial and administrative services);
- Intelligent surveillance and border security: focusing on technologies and capabilities to enhance the effectiveness and efficiency of all systems, equipment, tools and processes as well as methods for rapid identification required for improving the security of Europe's land and coastal borders, including border control and surveillance issues;
- Restoring security and safety in case of crisis: focusing on technologies providing an overview of and support to diverse emergency management operations (such as civil protection, humanitarian and rescue tasks), and on issues such as inter-organisational preparation, coordination and communication, distributed architectures and human factors.

The three **cross-cutting** areas / domains are:

- Security systems integration, interconnectivity & interoperability: Intelligence, information gathering and civil security, focusing on technologies to enhance the interoperability of systems, equipment, services and processes, including law enforcement, firefighting, civil defence and medical information infrastructures, as well as on the reliability, organisational aspects, protection of confidentiality and integrity of information and traceability of all transactions and processing;
- Security and society: mission-orientated research focusing on socio-economic analyses, scenario building and activities related to cultural, social, political and economic dimensions of security, communication with society, the role of human values and policy making, psychology of social environment of terrorism, citizens' perception of security, ethics, protection of privacy, societal foresight and systemic risk analysis. The research also addressed technologies that better safeguard privacy and personal liberties, vulnerabilities and new threats, as well as the management and impact assessment of possible consequences;
- Security research coordination and structuring: coordination of European and international security research and development of synergies between civil, security and defence research, improvement of legal conditions, and optimised use of existing infrastructures.

In addition, the Security theme also addressed two **other specific objectives**, which were elaborated in the relevant Work Programmes and calls for proposals. These related to International Cooperation and responding to emerging needs and unforeseen policy needs.

Finally, the Programme was required to contribute to several other contiguous **policy domains** and FP7 areas, including the implementation of EU external policies, the Common Foreign and Security Policy, the creation of an EU-wide area of justice, freedom and security, and to policy areas such as transport, health, civil protection, energy, development, and environment.

3.1.4 Programme implementation

The strategy for the implementation of the Security Research Programme was structured around three main **building blocks**:

- Capability projects aimed at building up and/or strengthening security capabilities required in the four security missions through the adaptation of available technology, as well as the development of security-specific technology and knowledge aiming at tangible results. The average duration foreseen for these projects was between two and four years, while the funding scheme was Collaborative Projects;
- Integration projects focused on a mission-specific combination of individual capabilities providing a security system and demonstrating its performance. They were based on technology and knowledge building blocks carried out within capability projects or elsewhere, had a length of four years and were funded via the Collaborative Projects scheme;
- Demonstration programmes were intended to carry out research activities aimed at large-scale integration, validation and demonstration of new security systems that were significantly beyond the state of art. They depended on the compatible, complementary and interoperable development of requisite systems and technology building blocks of the integration projects and capability projects;

The successful demonstration of the appropriateness and performance of novel solutions was considered a fundamental factor in the take-up of the output of the research conducted and its subsequent implementation under security policies and measures. As such, the **demonstration programmes** were seen as flagship initiatives of the FP7 Security Programme.

Their implementation took place in two phases:

- Phase 1 projects: focused on defining the strategic *roadmaps* and triggering Europe-wide awareness, involving end-users, industry and research. The roadmaps were meant to identify further research needs for Security theme integration projects and capability projects, but also for other FP7 themes or national programmes. These projects were funded under the Coordination and Support Actions schemes, with a duration of up to 1.5 years;
- Phase 2 projects: were designed to enable technical demonstrations of systems going beyond the state of the art, including certification and/or standardisation, development of marketable products and pre-procurement. The typical duration of phase two projects was up to four years under the Collaborative Projects funding scheme.

The structure of the Security theme reflects the specific challenges for security research. Security is a multidimensional issue; the solutions require interoperability, as well as cross-sectoral collaboration. The notion that large systems integrating subsystems of capabilities are best suited to address future security risks is reflected in the choice of an approach that is sequential in character, combines new uses of well-established and new technologies, and involves end-users and standardisation bodies.

The Security Research Programme was **operationally implemented** through annual Work Programmes. Six *Theme 10 Security Work Programmes* were published, one each year (apart from 2007 and 2008 when a joint Work Programme was published). There was a seventh call for proposals, which was a joint call between ICT and Security,[11] published in 2007. Only the programmes for 2011, 2012 and 2013 were focused on all seven of the mission-oriented and cross-cutting areas. The first three Work Programmes were more focused on demonstration programmes (phases 1 and 2).

The **Work Programmes** specified that cooperation between the user (authorities and organisations responsible for the security of citizens) and supply sides of security technologies and solutions should be a central feature of projects. Furthermore, projects were expected to include end-users within partnerships, in order to facilitate the development of appropriate solutions and increase the likelihood of further development and exploitation. There was also a request in the Work Programmes to embed in projects the awareness of their contribution to the security of European citizens and respect for fundamental rights and compliance with European societal values, including privacy issues.

The Work Programmes confirmed the **multidisciplinary nature** of the Security missions. They encouraged the development and use of technologies in a multi-purpose way, in order to maximise the scope for application and to foster cross-fertilisation. The testing, validation and demonstration of the security solutions developed in projects, involving the end-users as much as possible, was also considered at the core of the Security theme. Furthermore, standards were considered crucial for interoperability and take-up of results.

3.1.5 Programme activities and participation

FP7 calls for **proposals** started in 2007 and were published annually until 2013. They resulted in the submission of 1,790 eligible proposals, and a total requested EC contribution of €6.7b. Just over 300 of these proposals were subsequently retained (i.e. retained for negotiation), which corresponds to a ratio of eligible proposals to funded projects of 6:1.

[11] The interoperability and interconnectivity of supply systems is one of the cornerstones of the functioning of societies. The vulnerabilities in the intercommunication of systems, equipment, services and processes and their resilience against malicious attacks of terrorism and (organised) crime are fundamental concerns for the security of citizens. This is the main reason behind the introduction of an ICT–Security joint call. It aimed at funding research that would support protecting such critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.

Although the first FP7 security calls were issued in 2007, the first Security projects did not start until 2008. The number of projects starting has varied each year and has tended to increase over time, such that 56% of the total portfolio began in the years after 2012, compared with just 29% starting in the years 2008-2010. The last year saw the largest number of new Security projects, accounting for about one-fifth of the entire portfolio of projects.

In total, 307 projects were funded through the FP7 Security Programme over its lifetime. These involved over 3,700 individual participations and 1,824 *unique* organisations (participants). The total cost of all Security projects was €1.788b, with the EC contributing €1.263b (or 71%) of the total. The average contribution per project was €4.1m, and per participation was €338k.

The distribution of activities **across the mission areas** of the Security Programme was not even (see below). Three of the missions in particular accounted for an above average share of projects, participations and EC contributions: Restoring security and safety in the case of crisis, increasing the security of infrastructures and utilities, and increasing the security of citizens. They are marked in grey in the following table.

Table 6: Distribution of projects, participations and funding by mission

Missions	Projects	Participations	EC contribution
Security of citizens	18%	18%	19%
Security of infrastructures and utilities	17%	19%	20%
Intelligent surveillance and border security	10%	12%	17%
Restoring security and safety in case of crisis	18%	20%	23%
Security systems integration, interconnectivity and interoperability	10%	8%	8%
Security and society	15%	13%	9%
Security Research coordination and structuring	11%	11%	6%
(Other)	1%	0%	0%
Total	307	3,741	€1,263 bn

Source: Technopolis analysis of CORDA data, December 2014

3.1.6 Participation by mission area

Table 7 shows the distribution of participations by mission and by different types of actors. Overall, the highest share (43%) was from Private for Profit Organisations (excluding education) (PRC). Of this group, around half (49%) were SMEs (which accounted for 21% of all participations). Research Organisations (REC, 23%) and Higher or Secondary Education Organisations (HES, 21%) accounted for the next largest share of participations. Just 11% of participations were from Public Bodies (excluding research and education) (PUB), while the remaining 3% were from other types of organisation.

The overall numbers of participations are quite uneven across the four main types of actors (participating organisations), however, this reflects to a large extent differences in the size of the respective populations: the EU security community includes very many more businesses than it does universities or public institutions, for example.

The security research distribution does differ markedly from the distribution for FP7 overall, with a very much stronger engagement by larger businesses and public bodies, and a very much lower level of engagement with the higher education sector. The share of public institutions (many of which are end users) is especially notable, which is more than double the rate for FP7 overall.

Table 7: Share of different actors in Security Research mission participations

Mission areas	PRC	SMEs	REC	HES	PUB	OTH	Sum
Security of citizens	39%	(22%)	27%	22%	11%	2%	656
Security of infrastructures and utilities	55%	(20%)	20%	16%	6%	3%	710
Intelligent surveillance and order security	58%	(26%)	18%	14%	10%	0%	466
Security and safety in case of crisis	43%	(23%)	24%	20%	9%	5%	733
Security systems integration, interconnectivity and interoperability	48%	(25%)	21%	19%	8%	4%	295
Security and society	24%	(15%)	25%	39%	10%	3%	479
Security Research coordination and structuring	28%	(14%)	26%	16%	23%	7%	398
(Other)	0%	(0%)	25%	0%	75%	0%	4
Total Security	**43%**	**(21%)**	**23%**	**21%**	**11%**	**3%**	**100%**
Total FP7 (Cooperation and Ideas, excl. ERC)	**30%**	**(19%)**	**25%**	**37%**	**5%**	**3%**	**100%**
Total security participations	**1,609**	**(786)**	**860**	**786**	**412**	**112**	**3,741**

Source: Technopolis analysis of CORDA data, December 2014; Seventh FP7 Monitoring Report 2013

There is considerable variation in participation levels of different actors between the different **mission areas**, suggesting different parts of the Programme were more or less attractive to these actors. PRCs dominate in most mission areas (particularly 1-5), reflecting the higher participation rate of this group in the Programme as a whole. However, relative to their overall participation pattern, PRC involvement in three of the missions (2, 3, 5) is particularly high (shaded above). The sub-set of PRCs that is comprised of SMEs has relatively high participation rates in two of these missions (3, 5). Similarly, HES involvement is relatively high in just one area (6) and PUB involvement is relatively high in one area (7). REC participations are the most evenly spread across the different mission areas.

The following table highlights the mission areas that included some of the highest and lowest shares of participations from each of the four main types of participant.

Table 8: Mission areas with highest/lowest participation rates of different actors

Type (% of all participations)	Mission areas with a low % of participations from…	Mission areas with a high % of participations from…
HES (21%)	• Intelligent surveillance and border security (14%)	• Security and society (39%)
PRC (43%)	• Security and society (24%) • Security research coordination and structuring (28%)	• Intelligent surveillance and border security (58%) • Security of infrastructures and utilities (55%)
PUB (11%)	• Security of infrastructures and utilities (6%)	• Security research coordination and structuring (23%)
REC (23%)	• Intelligent surveillance and border security (18%)	• Security of citizens (27%) • Security research coordination and structuring (25%)

Source: Technopolis analysis of CORDA data, December 2014

3.1.7 Participation by different types of instrument

The Security projects used a range of different instruments. The table below shows the shares of projects and participations associated with each. Most projects (80%) used **collaborative research projects** (CP)[12] of one kind or another, while a much smaller share (19%) was funded by coordination and support actions[13] and a small minority (2%) used networks of excellence.[14]

[12] Collaborative Projects are those carried out by consortia with participants from different countries, aimed at developing new knowledge, new technology, products, demonstration activities or common resources for research. The size, scope and internal organisation of projects can vary from field to field and from topic to topic, from small or medium-scale focused research actions to large-scale integrating projects for achieving a defined objective.

[13] Coordination and Support Action Projects are focused on the support for activities aimed at coordinating or supporting research activities and policies (networking, exchanges, trans-national access to research infrastructures, studies, conferences, etc.).

The largest number of projects was funded through the CP-FP instrument for collaborative small- or medium-scale focused research projects. These projects also accounted for a third of all participations. Another 30% of projects were (generic) collaborative projects (CP), which also accounted for 34% of participations.

Table 9: Share of Security Research projects and participations by instrument

Instrument	Instrument	Projects	Participations
CP-FP	Collaborative small- or medium-scale focused research project	41%	34%
CP	Collaborative project (generic)	30%	34%
CP-IP	Large scale integrating project	8%	14%
CSA-SA	Coordination and support action – support action	12%	8%
CSA-CA	Coordination and support action – coordination action	7%	7%
NOE	Network of excellence	2%	2%
CP-CSA	Combined collaborative project and coordination & support action	0%	0%
Total		**307**	**3,741**

Source: Technopolis analysis of CORDA data, December 2014

The table below presents the share of participations in each instrument in terms of type of actor, and shows there is considerable variation in the **level of involvement**. Participation rates that are high relative to the overall participation rate of the group of actors are shaded. In particular, it is worth noting that HES and (to a lesser extent) REC involvement in networks of excellence is very high relative to their overall participation rate. REC participation in CSA-SA is also relatively high. Compared to their overall participation in the Security Research Programme, PUB actors are over-represented in CP-CSA and CSA-SA projects.

Table 10: Share of participations in each instrument by type of actor

Instrument	HES	PRC	(PRC-SME)	PUB	REC	OTH
CP	21%	47%	(20%)	8%	22%	2%
CP-CSA	0%	17%	(0%)	67%	17%	0%
CP-FP	24%	41%	(24%)	9%	23%	3%
CP-IP	16%	51%	(25%)	10%	19%	4%
CSA-CA	11%	25%	(10%)	31%	27%	6%
CSA-SA	15%	38%	(16%)	8%	31%	8%
NOE	49%	13%	(9%)	6%	30%	1%
All	**21%**	**43%**	**(21%)**	**11%**	**23%**	**3%**

Source: Technopolis analysis of CORDA data, December 2014

3.1.8 Participation by different types of organisations – 'participants'

The following table shows the shares of participations and EC funding by organisation type. The distribution of **EC contributions** by types of actors participating in the Security Research Programme broadly reflects the distribution of participations, with the main exception of PUB actors, whose share of EC contributions is less than half of their share of participations. This is reflected in the final column, which shows that the average EC contribution per PUB participation is ~50% of the programme average. By comparison, the slightly above average funding per participation for PRC and REC actors means that they account for a slightly higher proportion of funding compared to their share of participations.

Table 11: Share of EC contributions by different types of actors

	% of participations	EC Contributions	% of EC Contribution	Avg. EC Contribution per participation
HES	21%	€257,430,596	20%	€333,028
PRC	43%	€578,033,121	46%	€363,543
(PRC-SME)	(21%)	(€263,352,174)	(21%)	(€338,499)
PUB	11%	€63,850,743	5%	€162,058
REC	23%	€340,338,449	27%	€393,455
OTH	3%	€23,835,135	2%	€200,295
Total	100%	€1,263,488,044	100%	€337,741

Source: Technopolis analysis of CORDA data, December 2014

[14] Networks of Excellence support Joint Programmes of Activities implemented by a number of research organisations integrating their activities in a given field, carried out by research teams in the framework of longer term cooperation.

The rate of PUB and PRC participation in the Security Research Programme is considerably higher than for the Cooperation Programme overall (see the following table), while HES participation is relatively low. Indeed, while only 4.3% of participations in the Cooperation Programme overall relate to the Security Research Programme, the share of all PUB participations in the programme is more than double this rate (8.9%). The share of all HES participations in the Security Research Programme is much lower (2.7%).

Table 12: Participations by different actors – Security vs. Cooperation Programme

	HES	PRC	(PRC-SME)	PUB	REC	OTH	Total
Security Programme	21%	43%	21%	11%	23%	3%	3,741
Cooperation Programme	32%	35%	18%	5%	25%	3%	86,854

Source: Technopolis analysis of CORDA data, December 2014

The average EC contribution per PRC or REC participation is above the average for the Security Research Programme overall. It is also high compared to the average funding awarded to these types of actors across the Cooperation Programme. Funding per PRC participation is 23% higher in the Security Research Programme compared to the Cooperation Programme overall, while funding per REC participation is 10% higher. By comparison, average funding per PUB participation is 86% of the overall Cooperation Programme PUB rate.

There were 1,824 *unique* organisations participating in FP7 Security projects. Over half (51%) were private companies (PRC), 20% were higher education institutions (HES), 14% were public research institutes (REC) and 11% were public authorities or agencies (PUB). Each of these organisations, on average, received €692,702 in EC contributions.

With a total of 3,741 participations, the average number of participations per organisation is two. However, the participation rate of individual organisations is heavily skewed. The majority (1,194 or 65%) of organisations participated in only one project. At the other end of the scale, there are 53 organisations (3% of the total) that participated in eight or more security projects each (in one case, the number of participations is 82), and this small fraction of participants together accounts for nearly one-quarter of all participations in the programme (865 or 23%).

Table 13: Share of unique organisations participating in single or multiple projects

Number of participations	% of unique organisations
1	65%
2	17%
3	7%
4	4%
5	2%
6	1%
7	1%
8+	3%
Total	1,824

Source: Technopolis analysis of CORDA data, December 2014

3.2 Evidence Building Block 1: Rationale ("why")

3.2.1 Relevance of Security Research Actions

EQ1. Do the objectives of FP7 Security Research Actions correspond to the needs of EU stakeholders and were they adequately designed to contribute to the implementation of EU policies?
Key indicator: Ratio of value of EU contribution requested to EU contribution granted, overall and by mission

3.2.1.1 Overall

The conclusion on 'relevance' is that the general and specific objectives of the FP7 Security Research Actions correspond to the needs of EU stakeholders. This is confirmed through each of the data collection streams, from desk research and composition analysis to the participant survey and semi-structured interviews with stakeholders. Lastly, their continued relevance was unanimously endorsed by the experts attending the focus group (stakeholder) workshop.

Overall, the programme attracted 1,790 eligible proposals and funded 307 projects, a **ratio** of around six proposals to every approved project (KPI = 6:1), which is a good indication of the level of interest in and relevance of the Security Research Actions to the EU Security Research Community.

- The Security Research ratio is higher than the average for the Cooperation Programme overall (5:1) and demand outstripped supply as compared with all other Cooperation Programme thematic areas except social sciences (11:1) and ICT (7:1).
- The total requested EC contribution was €6.7b (€3.7m on average per proposal) and the contracted EC contributions totalled more than €1.26b, a ratio of about 5:1 and somewhat higher than the ratio for the Cooperation Programme overall.

The participant survey confirms that every one of the programme's six specific objectives is judged to be entirely relevant to one or more of the six categories of stakeholder by 40-60% of respondents. Certain objectives are of much greater relevance to one stakeholder group than another. For example, the programme's commitment to improve the competitiveness of the EU security industry is, unsurprisingly, judged to be relevant by 40% of all participants and of all industry participants; it is judged by a minority (17%) to be relevant to EU citizens. Developing the technologies and knowledge to ensure the security of EU citizens is the objective that is judged to be relevant by the greatest share of all respondents (60%), while industry competitiveness is the objective receiving the least widespread endorsement of its relevance.

The nine mission areas are also considered to be relevant to each of the six groups of EU stakeholders by 40-50% of all respondents to the participant survey. The security of citizens is the mission area that is most widely regarded as being relevant to most if not all of those stakeholders. Research coordination is the area that is judged to be relevant by the smallest share of respondents, with around 38% of all participants rating it as relevant. The mission areas and the programme are judged to be most relevant to EU policy makers and end-users, with notably narrower endorsement of relevance for the security industry and research base. Paradoxically, none of the specific objectives or mission areas is widely seen as being of particular relevance to SMEs.

The stakeholder interviews confirmed that the sense of a good fit with stakeholder needs holds **across each of the main stakeholder groups** consulted, albeit each constituency has a view as to how the programme might be re-oriented slightly to better fit their particular needs.

There is a general sense that end-users are at a rather early stage in their ability to articulate needs in terms of research due to their intrinsic concern with immediate operational issues, and as such the programme's focus is rightly broad and its emphasis on engaging users in demonstration and validation is also well regarded.

The only real point of disagreement that emerged within any of these conversations related to the issue of 'defence,' and a concern expressed by several interviewees (policy makers, industrialists and researchers) is that the Security Research Programme's strict focus on civil security applications is unduly restrictive and possibly counter-productive. Stakeholders argued that this has limited the programme's ability to deal with issues in a sufficiently coordinated manner and that it has also meant the programme has not fully grappled with what has been perceived as the greatest current threat to the security of EU citizens (terrorism).

3.2.1.2 Desk research

The **Group of Personalities (GoP)** on Security Research emphasised that the FP should follow a comprehensive approach to security research, that synergies should be pursued internally within countries (e.g. between police, fire, ambulance services) and externally (cross-border cooperation and security). In other words, it proposed the Security Research Programme should adopt a broad, holistic view of security[15] The FP7 SRAs have delivered on this.

The Interim Evaluation of FP7 Security Research[16] concluded that the objectives of the programme were entirely relevant to the needs of different stakeholders.

Over the course of its implementation, there have been several **adjustments to the scope** of the programme, reflecting the changing awareness of the needs of certain stakeholder groups, including the introduction of strengthening measures in 2011/2012 to improve the engagement of SMEs within the FP7 Cooperation Programme overall[17] and the launch of additional cross-cutting 'mission areas' to allow the programme to work more closely with key security organisations in third countries and in particular the United States.

The **CORDA database** shows that each of the FP7 Security Research Programme's seven calls for proposals attracted substantial interest from across the EU and from different stakeholders. As mentioned above, overall the programme attracted 1,790 eligible proposals and a total requested EC contribution of €6.7b (€3.7m on average per proposal), though the numbers vary significantly between calls and across years, as can be seen in the table below.[18]

Table 14: Distribution of proposals submitted and EC contribution requested by call

Call	Eligible proposals submitted		Requested EC Contribution	
FP7-SEC-2007-1	325	18%	€1,045 m	16%
FP7-ICT-SEC-2007-1	97	5%	€244 m	4%
FP7-ADHOC-2007-13	4	0.2%	€0.784 m	0,06%
FP7-SEC-2009-1	195	11%	€718 m	11%
FP7-SEC-2010-1	197	11%	€820 m	12%
FP7-SEC-2011-1	300	17%	€1,045 m	16%
FP7-SEC-2012-1	326	18%	€1,216 m	18%
FP7-SEC-2013-1	346	19%	€1,571 m	24%
Total	**1,790**	**100%**	**€6,658 m**	**100%**

Source: Technopolis analysis of CORDA data

Table 15 summarises the level of **demand** expressed for the Security Programme's calls in terms of proposals submitted, and compares this with the statistics recorded for the Cooperation Programme overall and its other constituent parts.

[15] Group of Personalities in the field of Security Research (2004) Research for a Secure Europe.

[16] CSES (2011) Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research. Sevenoaks.

[17] The measures aimed to create an environment that was more conducive to SME participation in FP7 projects. In the 2011 Work Programme, some 50 specific research topics were presented in order to increase the participation of SMEs, and in the Work Programme 2012 there were more than 90 research topics that specifically addressed SMEs. The strengthening measures were of various types, such as calls with broad and/or SME-friendly topics, streamlined application processes, making modest-sized consortia more eligible for funding, placing greater emphasis on close-to-market or demonstration activities, and the inclusion of specific criteria in calls, such as explicitly stipulating SME participation or SME coordination in projects, and output for the benefit of the participating SMEs. In addition, ring-fenced budgets for SMEs allocated a minimum share of the budget to participating SMEs.

[18] Similar data on the distribution of proposals by mission area is not available.

The data show that for every retained security proposal, nearly six were submitted (which is above the Cooperation Programme average of five), and three met the minimum quality threshold (also above the overall Cooperation Programme average). The table also shows that for every Euro of requested EC contributions in the retained Security proposals, €5.2 was requested by eligible proposals, which is above the €4.4 rate for the overall Cooperation Programme. The simple financial analysis suggests that the Security Research Programme's calls were highly relevant to the EU security community.

Table 15: Demand for Security Research and the FP7 Cooperation Programme

Programme Title	Proposals submitted for each proposal retained	Proposals above-threshold for each proposal retained	EC contributions requested for each €1 requested in retained proposals (€)
SSH	10.9	6.5	10.2
ICT	6.7	2.6	6.1
Food and Agriculture	5.5	3.6	5.6
Security (SEC)	5.9	3.0	5.2
Environment	5.3	2.9	4.8
Health	4.0	2.1	3.8
Energy	4.3	2.1	3.5
Transport	4.0	2.2	3.4
NMP	3.4	1.5	3.2
Space (SPA)	4.0	2.9	3.1
Joint Technology Initiatives	2.6	1.5	1.8
General Activities (GA)	1.3	1.0	1.1
Cooperation Programme	**5.1**	**2.5**	**4.4**

Source: Technopolis analysis of CORDA data

Table 16 shows the **distribution** of 3,741 participations in the FP7 Security Programme by **mission and type of actor**.[19] The participation rates differ across the four main types of actors; however, this is in part structural, reflecting the markedly different population sizes.

Overall, the highest share (43%, 1,609) of participations was from Private for profit organisations, excluding education (PRC). Around half (49%) of the PRC participations was represented by SMEs (21%, 786). Research Organisations (REC, 23%) and Higher or Secondary Education Organisations (HES, 21%) accounted for the next largest share. There is a broadly even split between public and private 'research' organisations. The level of engagement of end-users and public authorities is also revealed here: 411 participations (11%) were from Public Bodies (excluding research and education) (PUB), while the remaining 3% were from other types of organisations.

There is variation in participation rates across the different mission areas, suggesting that different parts of the Programme are more or less relevant to different types of actors. Industrial interest is strongest in surveillance and infrastructure, while universities favour societal issues. Research institutes are engaged at similar levels throughout the programme, reflecting their central role in the development and demonstration of these technologies and systems, while the public authorities are most heavily engaged in research coordination and structuring activities.

Table 16: Security Research participations, by mission and type of actor

Missions	PRC	SMEs	REC	HES	PUB	OTH	Total
1. Security of citizens	39%	22%	27%	22%	11%	2%	656
2. Security of infrastructures and utilities	55%	20%	20%	16%	6%	3%	710
3. Intelligent surveillance and border security	58%	26%	18%	14%	10%	0%	466
4. Restoring security and safety in case of crisis	43%	23%	24%	20%	9%	5%	733
5. Security systems integration, interconnectivity and interoperability	48%	25%	21%	19%	8%	4%	295
6. Security and society	24%	15%	25%	39%	10%	3%	479
7. Security research coordination & structuring	28%	14%	26%	16%	23%	7%	398
(Other)	0%	0%	25%	0%	75%	0%	4
Total	43%	21%	23%	21%	11%	3%	100%
Total Security Participations	1,609	786	860	786	412	112	3,741

Source: Technopolis analysis of CORDA data, December 2014

[19] This is the same table as Table 7 above, which shows the participation in the programme. In this case the same data is used to assess the relevance of the Security Research Actions.

3.2.1.3 Participant survey

After having examined the CORDA data to understand demand for the programme among organisations interested in security research, the evaluation team next focussed on the participant survey. Respondents were asked to indicate whether the objectives of the FP7 Security Research Programme are relevant to the needs of different EU stakeholders. This involved a complex question covering each of the programme's main objectives (e.g. improved competitiveness of the EU security industry) for each type of actor (e.g. end-user or security industry SME), and around 300 of our 700 respondents answered the question in full.

Table 17 presents the **results by type of actor** and for each specific objective. Respondents were invited to judge the relevance of each objective to each actor, and as such were able to provide multiple answers (votes); the columns show the number of times that each type of actor and objective was judged to be relevant by the respondents.

The results show that the **programme overall was judged to be widely relevant to industry**, policy makers and researchers. A slightly smaller share of respondents judged the programme to be wholly relevant to the needs of end-users and citizens.

At **the level of specific objectives**, the results show that each of the objectives is judged to be relevant to stakeholders' needs by a reasonable share of all actors in each category. The specific objective 'the development of knowledge and technology needed to ensure security' is most widely regarded – across actors – as being relevant to stakeholder needs. As may be expected, the distinctly industrial objective of 'improved competitiveness' is judged to be relevant to the needs of the security industry by a greater share of respondents as compared with its relevance to the security needs of EU citizens.

Table 17: Are the objectives of the FP7 Security Research Programme relevant to the needs of different EU stakeholders? (n = 708)[20]

Objectives	EU Security Industry (all sizes)	EU end-users	EU policy makers and regulators	EU research community	EU Security Industry (SMEs)	EU citizens	EU SMEs	Average across all actors
Develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters	67%	65%	61%	64%	46%	57%	35%	57%
Stimulate the cooperation of providers and users for civil security solutions	56%	59%	45%	44%	46%	32%	37%	46%
Ensure optimal and concerted use of available and evolving technologies to the benefit of European civil security	50%	57%	51%	42%	41%	44%	33%	45%
Deliver mission-oriented research results to reduce security gaps	48%	44%	49%	57%	36%	29%	28%	41%
Develop and strengthen capabilities, while respecting fundamental human rights including privacy	33%	44%	57%	40%	26%	60%	22%	40%
Improve the competitiveness of the European security industry	71%	24%	32%	40%	56%	17%	35%	39%
Average across all objectives	54%	49%	49%	48%	42%	40%	32%	45%

Source: Technopolis survey of FP7 Security Research participants, November 2014

Having asked participants about the relevance of the specific objectives, the project team went on to ask respondents to indicate whether they judged the mission areas of the FP7 Security Research Programme as being relevant to the needs of different EU stakeholders.

[20] Data shows the share of respondents indicating the relevance of a specific objective to each type of actor. Shading: Most regard as relevant (50%+); Many regard as relevant (40%+); Few regard as relevant (<40%).

Table 18 presents the results by type of actor (columns) and for each **mission area** (rows). This analysis produces a result that is different from the previous 'relevance' question, where the programme objectives were most widely judged to be relevant to industry. Within this analysis by mission, the overall programme is judged to be most widely relevant to policy makers and end-users. The relevance of the individual mission areas is more variable, and coincides with the more or less direct relationship between the focus of a mission area and given stakeholder group: security of citizens is most widely judged to be relevant to EU citizens.

These two questions were also included within the subsequent dedicated survey of end-users. As noted already, more than 90% of the respondents had participated in an FP project or network and were mostly very familiar with FP7 Security Research objectives, and as such it was pleasing to find that the balance of opinion as regards mission priorities coincided almost exactly with the feedback from the end-users within the participant survey.

Table 18: Are the mission areas of the FP7 Security Research Programme relevant to the needs of different EU stakeholders? (n = 708)[21]

Mission areas	EU policy makers and regulators	EU end-users	EU Security Industry (all sizes)	EU research community	EU citizens	EU Security Industry (SMEs)	EU SMEs	Average across all actors
Security of citizens	63%	61%	47%	47%	79%	38%	26%	52%
Security of infrastructure and utilities including networks	58%	60%	62%	43%	47%	43%	32%	49%
Security and society (cross-cutting)	62%	57%	40%	45%	67%	29%	26%	47%
Security and safety in case of crisis	62%	60%	44%	37%	62%	31%	24%	46%
Security systems integration, interconnectivity and interoperability	49%	51%	66%	43%	28%	45%	30%	45%
Intelligent surveillance and border security	62%	51%	49%	36%	47%	38%	21%	43%
Security research coordination and structuring	49%	35%	42%	66%	18%	34%	22%	38%
Average across all mission areas	**60%**	**52%**	**49%**	**48%**	**46%**	**37%**	**26%**	**45%**

Source: Technopolis survey of FP7 Security Research participants, November 2014

3.2.1.4 Stakeholder interviews

The results of the stakeholder interviews were **consistent across all groups**, with the great majority of interviewees holding the view that the objectives of the FP7 Security Research Actions did correspond to the needs of EU stakeholders at the launch of the programme and continue to do so today.

DG HOME staff (previously DG ENTR), unsurprisingly, affirmed that the programme's objectives were entirely relevant to the needs of various EU and MS stakeholders. Officials at other DGs had a rather narrower view of the Security Programme's objectives; however, they were in all cases supportive of those objectives (e.g. Environment [DG ENV], Maritime Affairs and Fisheries [DG MARE], Migration and Home Affairs [DG HOME], Humanitarian Aid and Civil Protection [DG ECHO] and Mobility and Transport [DG MOVE]).

Interviewees from **Member States** expressed similarly positive views about the programme, noting the growing importance of civil security issues and the very limited funds available nationally to work on these topics. There was general support too for the scope of the programme. The only substantive remarks related, first, to the need to support more fundamental research and, secondly, a desire to see a change in the balance in priorities between the security of citizens and the competitiveness of the security industry. There was a concern that these two broad objectives were sometimes in tension and that the ownership of the programme by DG ENTR had meant that the primary focus was on industry, whereas these contributors felt it ought to be on the citizen.

[21] Data shows the proportion of respondents indicating relevance of a specific objective to a type of actor. Shading: Most regard as relevant (50%+); Many regard as relevant (40%+); Few regard as relevant (<40%).

Industry partners also expressed positive views about the relevance of the programme's objectives to the research and technology needs of the security industry; however, there were reservations expressed about the absolute suitability of the FP model as a means by which to support industrial innovation. The innovation lifecycle of many aspects of the security sector is 2-3 years, whereas the FP has a lifecycle that is closer to five years from conception of the call to completion of projects, double the periodicity found in industry. One senior industrialist remarked that as we cannot easily change the nature of the FP, it perhaps makes more sense to focus on more fundamental issues where progress may well benefit from the longer gestation period and ability of these innovation platforms to convene larger groups.

Academic contributors were strongly supportive of the need for an EU research programme and broadly positive about the relevance of the FP7 objectives to the needs of the security research community. There was a single widely expressed reservation: the decision to focus on very applied, near-term projects made the calls a little more relevant to industry and end-users and a little less relevant to the interests of the public research base. The academic community would have preferred more opportunities for carrying out rather more fundamental research.

In contrast to the academic discussion partners, **EC officials** interviewed were rather positive about the programme's commitment to focus on shorter-term issues, which more closely reflect their operational realities. Several commentators stated that the programme would have been more relevant to end-users if it had been even more sharply focused on developing and demonstrating real-world solutions. "Interoperability challenges – technical and institutional – are legion, and there is a long road to travel between a promising new technology and an implementable solution." At the same time it was acknowledged that FP7 and Horizon 2020 are applied research programmes, which work in a 5-10 year time horizon. Hence, they cannot meaningfully respond to specific events such as terrorist attacks or natural disasters, even if EC or MS policy makers want to be able to better address their pressing, short-term priorities, triggered by such events. This is, on the other hand, not to say that EU RTD FP strategies and work plans should be fixed and immutable, but to recognise that these instruments have a particular quality and functionality.

A majority of contributors believe that the Security Research Programme has made good progress in its ambition to **engage end-users**, and while the interaction is a long way from perfect, the intent is clear and the direction of travel positive. Interviewees believe the Security Research Programme has been rather more successful than other parts of the FP7 Cooperation Programme in this respect. The interviewees from **DG MARE and DG MOVE** were both quite complimentary about progress, and noted the extent of the underlying challenge in face of the diversity of end-users and the lack of their coordination, even within EU Member States. Often there are no structures by which any third party might simply and clearly engage with what are quite large and diverse communities. End-user engagement has been facilitated where there were other EU policies implemented in the recent past, which had already galvanised interest and led to the creation of fledgling networks and coordination groups (e.g. EU Maritime policy).

While a majority of stakeholders were of the opinion that the programme addresses the most pressing **needs of EU citizens**, several stakeholders pointed out that this role was often not visible to the public. "I would say, yes [the programme addresses the needs of EU citizens], but citizens do not know about it!" The example of water might serve as a case in point. While most people appreciate to swim in clean water during their holidays and while industry needs safe and secure waters for production and trade[22], most citizens are not aware that EU Security Research is concerned with the protection of these resources.

One interviewee singled out the 'Driving Innovation in Crisis Management for European Resilience' (DRIVER) project[23] as an example of a rather important mechanism for bringing together the crisis management community. This €46m demonstration project involves a consortium of 37 partners from across the EU and includes the end-users, authorities, industry and research groups.

[22] One interlocutor pointed out that 75% of EU trade (90% if trade through pipelines is included) depends on free and safe sea-lanes.

[23] http://cordis.europa.eu/project/rcn/188608_en.html

Another interviewee noted the important contributions being made by FP7 to the EU's commitment to create an Integrated Maritime Surveillance (IMS) system,[24] with multiple projects (e.g. PERSEUS[25]) having supported progress in realising the European roadmap for CISE (Common Information Sharing Environment). There have been challenges along the way, resulting in rather slower progress than anticipated in realising an EU IMS,[26] and the EU CISE 2020 project (€12.5m) launched following the final FP7 call for proposals (2013) is expected to validate different elements of the proposed interoperability framework and support incremental implementation of CISE.

There were several **specific topics** that were mentioned as possibly representing important gaps in the programme's topic coverage (not its missions or objectives), including the issue of the proliferation of drones/UAVs beyond the military and the potential threat that this technology poses as a weapon that may be deployed by terrorists. Other interviewees remarked on the disjuncture between research and policy and politics, and asked whether more could be done to develop instruments that might better bridge this perennial gap.[27]

Yet another topic that was inadequately addressed is **societal resilience**. The topic of societal resilience has emerged as an important notion for the security area and for security research in the progression from FP7 to the Horizon 2020. While FP7 Security Research Actions focused on hardware, societal resilience is now firmly included in the research agenda. As it will never be possible to avoid all risks, a certain tolerance of risk among citizens will have to be maintained, which explains the need to strengthen societal resilience. As one interlocutor put it: "Resilience does not only include an 'ability to bounce back' to normal patterns once a crisis or attack has occurred, but also the ability to absorb shocks and to deal with it at decentralised and local level. It is increasingly necessary for society to be prepared to deal with natural disasters, for example. The Department of Homeland Security (DHS) in the US has done a great job, trying to make people in crises not dependent on being rescued (self-awareness, preparedness). One might also mention the (laudable) attitude of Londoners following the 7/7 bombings and the public's 'unwillingness to be terrorised' with people returning to work and making full use of the transport system the day after the atrocities. The mission of Restoring in Case of Crisis addresses part (but not all of the issues of resilience)."

The great majority of interviewees had a limited view about the design of the Security Research Programme's objectives and the process by which different stakeholder groups had engaged in any kind of dialogue or definitional activity. One contributor however felt the process lacked transparency, and that the influence of the Member States over the programme's content was perhaps too great, given the fact this is an EU instrument. The Lisbon Treaty (2007) strengthened the role of the Commission within the realm of civil security, defining it as an area of 'shared competence' where previously it had been a matter for Member States. There is undoubtedly a learning curve that will take time to scale, as the EU and MS come to a practicable understanding of what subsidiarity means in this context.

3.2.1.5 Case studies

The team also considered the issues of relevance and programme design in the selection of case studies, including consideration of the complementarity of CBRNE research and projects involving the European Defence Agency (EDA), port security and the engagement of citizens in the security research programme. The case study summaries can be found in this report in Appendix E, with the full case studies presented in Appendix F.

---

[24] European Commission (2010) Integrating Maritime Surveillance – Common Information Sharing Environment (CISE), Brussels: European Commission.

[25] http://cordis.europa.eu/project/rcn/97515_en.html

[26] See the 2014 commentary, 'The Successes and Failures of the European Union Integrated Maritime Policy: Critical Mid-term Review 2007-2013,' published in the Journal of Contemporary European Research, Volume 10, Issue 3 (2014). Marin Chintoan-Uta, European Maritime Safety Agency (EMSA).

[27] The large-scale integrated project (€35m) FP7 Security project, End-user driven DEmo for cbrNe (EDEN), organised an event specifically on this topic, which was widely supported: Strengthening Science-Policy-Industry links in the CBRN-E sector Brussels, 30 January 2014.

The **EDA case study** provides a good and reassuring account of the programme's willingness to work with other agencies that have a strong interest in security research, in order to guarantee there is a high degree of coherence between them and a minimum of unnecessary duplication. Using the example of research on how to address chemical, biological, radiological, nuclear and explosive (CBRNE) hazards, the case study shows how the EDA and the EC have coordinated their activities in this field.

Coordination activities have taken place between the EC and EDA since the latter was established in 2004. However, the 2011 European Framework Cooperation (EFC) on Security and Defence Research marked a significant change in cooperation. This agreement sought a more systematic synchronisation between the research and technology investments of the EDA and EC, so as to maximise complementarities and synergies of civilian security, space and defence-related research programmes. Therefore, within the limits imposed by legislation, the EC and the EDA have established a communication and cooperation channel that serves as a good first step in the direction of tackling common threats and risks in a coherent and coordinated way, with the overall objective of ensuring citizens' security. Some stakeholders consulted for this case believe that this should be developed further during H2020, with involvement in more relevant projects and activities.

Given the ultimate focus on the security of citizens, the programme has been scrutinised and challenged in its early years as regards the sufficiency of its **engagement with citizens.** It is fair to say the programme did not work closely with individual citizens in defining its agenda or indeed as a required 'voice' within individual projects. It is also clear from the interviews and desk research that the programme has made progress with its public engagement, giving more weight to the issue within the standard ethical review process. This has resulted in the increasing involvement of civil society organizations (CSO) within project consortia and increasing efforts to involve individual citizens directly in project focus groups and validation workshops. There is arguably more that could be done in engaging citizens upstream in discussions about the focus of future Work Programmes, probably through a more conscious commitment to include CSOs within the various agenda-setting fora and events.

3.2.2 Coherence of the intervention logic

EQ2. To what extent did the objectives reflect (was there a clear intervention logic between) the levels, Specific Programme and Work Programme activities?
Key indicator: Balanced distribution of participations and EC contributions, among objectives

3.2.2.1 Overall

Considering the description of the objectives and the rationale for the Security Research Actions, as set out in the Council Decision on FP7[28], the evaluation team judged that there is a **coherent intervention logic** between the levels of objectives and the Work Programmes.

3.2.2.2 Desk research

The intervention logic (Appendix H) provides an overview of the scope of the Security Research Programme. Table 19 provides an overview of the **coverage of the programme's calls for proposals** by mission and by type of instrument, and shows that all mission areas have been addressed on multiple occasions since the beginning of the programme. Not every Work Programme has issued calls for proposals for all types of FP7 projects; for example, demonstration projects appear only in certain years and not for all mission areas. Each of the four main mission areas was addressed in each annual Work Programme. The cross-cutting missions were pursued in a consistent manner only in the latter half of the programme.

[28] Decision No 1982/2006/EC.

Table 19: Overview of FP Security Research, by Work Programme (WP), Instrument and Mission

		Main Security Missions				Cross-Cutting Missions		
Work Progr.		**Security of citizens**	**Security of infrastructures and utilities**	**Intelligent surveillance and border security**	**Restoring security and safety in case of crisis**	**Security systems integration, interconnectivity and interoperability**	**Security and society**	**Security Research Coordination and structuring**
2007/08	Demonstration Projects		X	X				
	Integration Projects	X	X	X	X			
	Capability projects	X	X	X	X			
	Coord. & support actions						X	X
2009	Demonstration Projects	X			X			
	Integration Projects	X	X	X	X			
	Capability projects	X	X		X			
	Coord. & support actions	X	X		X		X	
2010	Demonstration Projects		X	X	X			
	Integration Projects	X		X	X			
	Capability projects	X	X		X			
	Coord. & support actions	X	X		X		X	X
2011	Demonstration Projects							
	Integration Projects	X	X	X	X			
	Capability projects	X	X	X	X	X		
	Coord. & support actions	X			X			
2012	Demonstration Projects							
	Integration Projects		X	X	X	X		
	Capability projects	X	X	X	X	X	X	X
	Coord. & support actions		X	X	X	X	X	X
2013	Demonstration Projects							
	Integration Projects	X			X	X		
	Capability projects	X	X	X	X	X	X	X
	Coord. & support actions	X	X	X	X		X	X

Source: Technopolis analysis of Work Programmes

Table 20 shows the distribution of projects, participations and EC contributions across the four main security missions (1-4) and three cross-cutting missions (5-7). The analysis shows that each **mission area has supported a significant number of projects**, though there is a degree of variability across the seven mission areas, with the numbers of projects funded falling in the 10-20% range. The spread for participation levels is somewhat larger, at 8-20%. There is more variability in funding levels, with each of the seven mission areas accounting for 6-23% of the €1.26b in total EC contributions, varying between €75m (research coordination) and €290m (restoring security).

Table 20: Distribution of projects, participations and funding by mission

Missions	Projects	Participations	EC contribution
Security of citizens	18%	18%	19%
Security of infrastructures and utilities	17%	19%	20%
Intelligent surveillance and border security	10%	12%	17%
Security and safety in case of crisis	18%	20%	23%
Security systems integration, interconnectivity, interoperability	10%	8%	8%
Security and society	15%	13%	9%
Security Research coordination and structure	11%	11%	6%
(Other)	1%	0%	0%
Total	307	3,741	€1.26b

Source: Technopolis analysis of CORDA data

Information on indicative budgets per mission area was not available for this study, and so the extent to which the distribution of projects and funding across the programme reflects the expected / intended distribution could not be assessed.

3.2.2.3 Stakeholder interviews

From the discussions with various interviewees and other stakeholders emerged the overall impression that the mission areas were a **good fit** with the community's wider research and knowledge requirements and that there had been a reasonable balance of investment across the seven mission areas. Thus, the stakeholder interviews confirmed the view gained from the desk research.

A small minority of interviewees **questioned the clarity**, if not the coherence of the programme's matrix structure, with thematic priorities sitting alongside cross-cutting issues. However, for each of the commentators who argued that the programme should simply have focused on the thematic areas, another interviewee complimented the Commission Services on the decision to include the cross-cutting issues and in particular the security and society topic.

3.2.3 The extent to which projects met their objectives

EQ3 To what extent did FP7 Security Research Actions meet their objectives?
Key indicator: % participants that judge their project to have delivered fully on its objectives

3.2.3.1 Overall

The participant survey strongly suggests that the majority of FP7 Security Research Actions met their objectives in full at the level of individual projects.

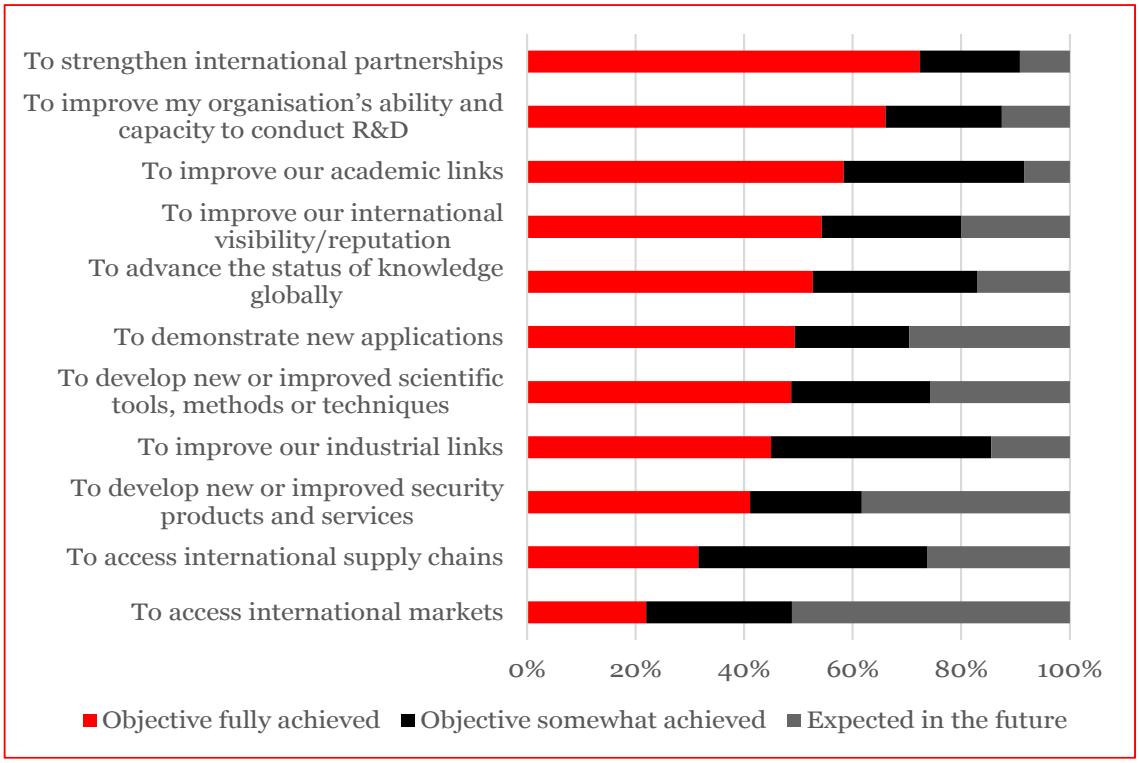
This positive finding is echoed by the analyses of results from the Commission's project-monitoring system (SESAM), which show that around 38% of the 61 completed and fully processed Security Research projects were judged by their project officers and external peer reviewers to have met their project objectives in full. This ratio is, however, lower than a comparable ratio for the FP7 Space Research Programme, where 51% of the Collaborative Projects and 42% of the Coordination and Support Actions were deemed to have fully achieved their objectives.

3.2.3.2 Participant survey

Participants were invited to indicate whether their project had targeted one or more of a series of 10 generic objectives (e.g. advance the status of knowledge) as well as signalling the extent to which their project had met that objective or was likely to do so in the future.

Figure 4 presents the results for all participants, suggesting that stronger international partnerships, new insight and understanding, and new applications were objectives for around 80% of all Security projects and that the project objectives had been realised in full in 50-75% of those projects where it was a goal.

Figure 4: Which of the following elements were objectives of the project, and to what extent have they been achieved (or are likely to be achieved in the future)? (n = 599)



Source: Technopolis survey of FP7 Security Research participants, November 2014

There were a number of **significant differences** in the responses given by project coordinators as compared with those made by project partners, so the figure shows the results for all respondents: coordinators were somewhat more positive about the achievement of improved industry-academic links, as compared with all participants, and project partners were most positive about the realisation of objectives relating to new tools and techniques. These outcomes would seem to be a natural reflection of the different perspectives and roles of the two groups, with project coordinators being better placed to judge impacts on networks and partners being better placed to judge the achievements around new tools and methods.

There were suggestions from the respondents to include improved knowledge, information flows and relationship between end-users and innovation providers among the objectives. A greater share of end-users reported that their objective to "improve the organisation's ability and capacity to conduct R&D" had been achieved, as compared with responses from participants overall. This latter objective was less widely reported as being of importance to industry or research participants –perhaps understandable, as these participants have a longer history of security research – and therefore represents a positive contribution by the programme to the desired improvement in research capacity among end-users.

3.2.3.3 Desk research

As of the end of December 2014, 102 of the 307 Security Research projects had submitted final reports and 61 of those projects had been fully processed with all final outputs recorded within the Commission's SESAM project monitoring database. This partial dataset, comprising projects from the earliest calls and those of shorter duration, nonetheless allows gaining an overview of the kinds of results the programme is going to deliver overall.

The SESAM database includes a field that records the extent to which every completed and processed project was judged to have met its objectives. This judgement is made by the project officer based on project deliverables and peer review reports; the appraisal comprises four gradations, from fully 'achieved its objectives' to 'failed.' Of the processed projects:

- Over one-third (38%) were assessed as '**fully achieving objectives'** and / or delivering 'expected results' with significant immediate or potential impact (even if not all of the objectives mentioned in the technical annex were achieved);
- Over half (56%) were assessed as 'achieving **most** objectives' with relatively minor deviations;
- Three projects (5%) were assessed as 'achieving **some** objectives,' however corrective actions will be required;
- Just one project (2%) has so far been assessed as '**failing** to achieve critical objectives' and is severely delayed.

While the number of projects assessed in individual mission areas is as yet quite small, at least half of those in three of the mission areas have been assessed as 'fully achieving objectives': these are 'restoring security and safety in case of crisis', 'security research coordination and structuring', and 'security systems integration, interconnectivity and interoperability'. In the other four mission areas, the proportion is less than 40% in each case.

SESAM also records information about other types of project **achievement**, which show that for the 61 Security Research Projects:

- 31% had involvement of non-RTD actors;
- 23% had an impact on EU policies;
- 18% had good innovation potential;
- 18% had high visibility / were media attractive;
- 11% had a highlighted success / case story;
- 8% had substantial R&D breakthrough character;
- 7% were linked to R&D national / international programmes;
- 5% had outstanding use / exploitation of results;
- 2% had an impact on promoting Joint Programming;
- 0% had significant R&D participation from outside the EU.

3.2.3.4 Stakeholder interviews

The results of the stakeholder interviews were more difficult to synthesise, as their **views varied**. Those contributors with close proximity to individual projects generally expressed positive views about the progress that was made and believe the programme has worked well overall. Those interviewees with a more strategic or broad-based view of security issues were rather less sanguine, and many argued that security is worsening in Europe and that the research programme is not obviously helping governments and security agencies to do a better job in the face of extremism or illegal immigration, to name two topics. There was also a widespread view that more ought to be done to ensure project results are shared more widely and properly exploited.

3.3 Evidence Building Block 2: Implementation ("how")

3.3.1 Implementation of FP7 Security Research Actions

EQ12. Were FP7 Security Research Actions implemented in an efficient way?
Key indicator: % participants that judge the programme to have been implemented efficiently; share of stakeholders that judge the programme to have been implemented efficiently

EQ13. Are there major differences between the mission areas of FP7 Security Research? Are there differences as regards FP7 project types?
Key indicator: Variance across mission areas in the % of participants that judge the programme to have been implemented efficiently; variance in the balance of participant opinion on efficiency across types of actors (e.g. end-users, industry, etc.);

EQ16. What aspects of FP7 Security Research are the most efficient or inefficient, especially in terms of resources mobilised by stakeholders?
Key indicator: Time-to-grant statistics ranked against the other areas of the Cooperation Programme; variance in the balance of participant opinion on efficiency across types of projects (e.g. research, support actions, etc.)

3.3.1.1 Overall

In general, FP7 Security Research Actions were implemented efficiently, and compare reasonably well overall with the other areas of the Cooperation Programme.

The participant survey revealed that **30-70% of participants are very satisfied or satisfied** with the implementation of the Security Research Actions, with the proportion increasing to 70-90% when adding participants stating they are neither satisfied nor dissatisfied.

The results show that there is widespread satisfaction within the EU Security Research community with the programme's basic design and information provision (e.g. the amount of funding earmarked for projects, time allowed for submission, information about the programme and calls for proposals, etc.). Programme information, financing levels, and submission timetables are all well regarded by the great majority of participants. The Commission's new ICT systems and participant portals are also judged to function reasonably.

However, there is no doubt that the **single biggest source of frustration is the time-to-grant (TTG) performance** of the programme, which at 526 days on average is 1.5 times longer than the average TTG figure for the Cooperation Programme overall.[29] This differential is however largely a function of the different process the security programme had to follow as compared with the rest of the Cooperation Programme: Appraisal = (i) scientific/technical proposal evaluation (ii) ethical screening/review and then (iii) the additional Security Scrutiny[30] to identify any projects that would need to be run as classified projects managed by the security policy team in DG HOME rather than by REA.[31]

[29] Time to grant (TTG) is the time elapsed from the deadline of the call for submission of proposals until the signature of the grant agreement.

[30] The Security Scrutiny is a standard procedure, foreseen for security research proposals by the "Evaluation Rules" and the "Guidelines for Applicants".

[31] Under FP7 (2007-2013), DG ENTR was responsible for the research activities in the fields of Security Research and Space Research. The implementation of calls and grant agreement management is partly delegated to the Research Executive Agency (REA). While DG ENTR was responsible for all projects involving classified information and projects

Negotiation of classified projects can take many months as it often places requirements on contractors that they cannot easily address and some further preparatory work is required on their part (e.g. security of their facilities).

The TTG statistics show a high level of variability in the average time-to-grant across calls; however, it is important to understand that this is driven in large part by differences in the size of the calls and the number of proposals that had to be processed and contracted.

The survey results revealed no significant differences in respondents' views about management **efficiency** across **mission areas**.

The interviewees mentioned differences in 'efficiency' between **project types**, with the largest projects taking proportionately more time to process than smaller projects. There was also an issue involving cooperation with SMEs, given the relatively greater effort that was required to test the robustness of engagement within consortia and the nature of the planned contribution. These differences are common to all areas of the FP7 Cooperation Programme and are not specific to the Security Research Actions.

The programme has strengthened its attention on **societal issues** across successive calls for proposals. This is partly a reflection of a more general push within the Commission, led by the responsible Services within DG RTD, to ensure that all applications give due consideration to research ethics, but it has been an issue for security in particular. The Security Research Programme was criticised in the press for being too technocratic, and this led to a re-appraisal of both the sources of advice used to inform the development of Work Programmes and project-level assessments. This is not an easy transition to make, as security researchers were rather unfamiliar with the ideas and how they might work in practice; however, the Commission has persevered and now has a good number of specialists available to carry out ethical screenings and reviews of security proposals (including for Horizon 2020). In addition, FP7 projects were asked to include project advisory bodies providing advice on such challenges to the researchers.

All FP7 proposals are subject to **ethical screening** to determine whether a proposal warrants a full ethical review, either by default, because it involves a certain type of research activity (e.g. research with children), or where the peer reviewers judge the project to include a higher risk activity for whatever reason and as such recommend it is looked at more closely in a full ethical review carried out by ethics specialists.

A **dedicated case study** has been carried out on ethics in FP7 security research.[32] It was found that around 10% of all FP7 proposals and 25% of all security research proposals have been subject to ethical review, reflecting the degree to which security research will tend to address issues that have a wider ethical dimension, like surveillance systems and privacy.

Views on this subject were also obtained from the stakeholder interviews, focus group (stakeholder) workshop discussion and case study interviews, revealing that the ethical screening/review process generates **mixed views**, with some arguing that it is just another bureaucratic procedure that has made no material difference to the projects in question, simply confirming they are appropriately designed. Others argue that the ethical screening/review process has given proposal developers pause for thought when formulating project ideas (better by design), while the resulting Ethical Screening /Review Reports have reportedly led to small but useful refinements to project designs, implemented as part of the contract negotiations.

Under FP7, more and more projects have created project-level ethical review boards or appointed specialist advisors in order to provide on-going advice to project teams helping address challenges as they arise during the course of a project. It is also worth noting that participants had some comments regarding the burden of completing the ethics **'checklist'** that is included within proposal templates, and asked whether this overall process might be made a little smarter and simpler.

---

with direct and high political relevance, REA was responsible for the call management and related proposal evaluation as well as for managing the majority of projects (i.e. those not subject to EU Classified Information [EUCI] rules).

[32] For the executive summary and the complete case study see Appendix E and Appendix F respectively.

The programme has also supported a very small number of projects looking at the ethical dimensions of security research, but these sat awkwardly in the Work Programme and the 'ethics' projects were considered to be orphans in the portfolio.

3.3.1.2 Desk research

The **average TTG figure** (526 days) for the Security Research Programme is substantially higher than the average figure for the Cooperation Programme overall (333 days), as well as more than double the current target for Horizon 2020.

This figure may reflect the inexperience of at least some fraction of the applicant base, since this was effectively the first Security Research Programme. However, the major factor is likely to be the **additional Security Scrutiny** procedure, which is required of security research proposals.

Across the Security Programme,[33] TTG varied between 228 days and 929 days (approximately 8-31 months), with an average of 526 days (~18 months). As can be seen in the table below, which shows the results by call, the joint SEC-ICT call in 2007 had the highest average TTG (636 days).

Table 21: Time to grant statistics for FP7 Security Research Actions in days

Call	Average TTG	Minimum TTG	Maximum TTG
FP7-SEC-2011-1	458	363	743
FP7-SEC-2013-1	495	455	566
FP7-SEC-2007-1	524	228	929
FP7-SEC-2010-1	526	386	764
FP7-SEC-2009-1	548	382	679
FP7-SEC-2012-1	600	391	761
FP7-ICT-SEC-2007-1	636	467	747
Overall	526	228	929

Source: Technopolis analysis of CORDA data

For the Cooperation Programme as a whole, the average TTG is 333 days.[34] This is significantly shorter than the Security Programme average. However, in Horizon 2020, the Commission has set a target of 240 days for TTG, which is below the FP7 Security average (indeed, only three projects would have fallen within this target).

3.3.1.3 Participant survey

The figure below presents the results of a question put to all participants, inviting respondents to indicate how satisfied they were with the implementation of 15 different aspects of the FP7 Security Research Actions that ranged from the provision of information about calls for proposals to the user-friendliness of the Commission's new ICT tools.

The results show there is **widespread satisfaction** among the EU Security Research community with the programme's basic design and information provision (e.g. the amount of funding earmarked for projects, time allowed for submission, information about the programme and calls for proposals, etc.).

For five of the 15 implementation 'aspects,' less than half of the responding participants stated that they were 'satisfied' with the dimension in question. Programme success rates (20%) and project reporting requirements (18%) were both sources of dissatisfaction. There is no mistaking the single greatest source of frustration, however, which is the time-to-grant performance of the programme, causing more than 30% of respondents to signal their dissatisfaction.

[33] Projects funded through the FP7-Adhoc-2007-13 call have been excluded – as this was a rolling call, with most projects starting before the final call closure date in 2013.

[34] Based on 23,218 projects, which excludes calls with projects starting before call closure and any projects with missing date information.

Figure 5: How satisfied or dissatisfied were you with the following aspects of the FP7 Security Research project cycle and its implementation? (n = 585)

Source: Technopolis survey of FP7 Security Research participants, November 2014

Looking at the results for different **types of participants**, it can be said that in general more project coordinators are satisfied with programme implementation than are other participants. There is no significant difference in the 'ranked order' of the various implementation aspects; however; participants are rather less widely supportive of the Commission's processes, and in particular more than 50% of respondents were dissatisfied with time-to-grant performance.

Lastly, when comparing the results for **end-users** and non-end-users, there are few significant differences, beyond two rather interesting points: it is evident that a greater proportion of end-users is satisfied with support for project commercialisation and with IP management as compared with all other participants.

In addition to rating programme implementation, survey respondents were asked to describe any element that was **in need of improvement**, and why.

Based on several hundred free-text **comments from participants**, every aspect of the programme's design and implementation, ranging from the clarity of the rules on eligible costs of projects to the number of languages in which the call text is made available through to expected project duration, was challenged by at least one respondent.

The most widely recorded complaints quite naturally echoed the results of the ranking exercise shown above, with several tens of respondents recommending that the Commission look to improve matters in the future regarding each of the following items, which are listed in descending order of frequency of comment:

- Time-to-grant: TTG is considered too long, and creates problems for projects and project consortia. If it takes one or two years to launch a project, it is quite likely that the focus of the project – its technical objectives – may have become less relevant to some or all members of the consortium, and that one or more partners may have had to change the level of their commitment to the project as a result of other events outside the project;
- Project reporting: The project reporting requirements are considered to be too detailed and too complicated, with multiple data requests that didn't seem especially relevant. The burden of addressing these requests can be a source of friction within project teams as well as a source of delays in project progress as coordinators negotiate with officials about the completeness and correctness of their reports. Somewhat contrarily, several project coordinators suggested that the project reporting requirements were inappropriately balanced, and that more weight should be given to qualitative feedback;
- Proposal success rate: The success rate is too low. This makes it harder to build consortia, and favours established players. It also means that organisations may try once, and even though they have written a good proposal and built a solid partnership, the amount of money available means they have little chance of winning a grant. This can be a disincentive for organisations that are less familiar with FP research;
- Responsibility for commercialisation: The need to improve support for commercialisation is emphasised, in particular for SMEs.

Among the comments from coordinators were those that the programme was originally well conceived and well financed, and, in general, well managed administratively. There were, however, **small numbers of quite critical remarks**, which warrant further reflection. These included the following: "technical implementation needs serious improvement"; "risk is mostly avoided"; "new players are prevented from participating by the capitalisation of the programme by impenetrable alliances"; "evaluation [review] is inconsistent"; and "topics either are written by a single hand or incomprehensively fused into a hodgepodge in an attempt to encompass everything".

3.3.1.4 Case studies

There is no dedicated case study on the question of administrative efficiency. However and given the importance of this instrument for the security community, this evaluation includes a case study on the programme's use of demonstration projects[35] that provides useful insights.

The **evaluation team commends** the approach taken in the development of demonstration projects, with a two-phase approach allowing security communities to come together to carry out strategic roadmapping exercises in the first phase and to use these priority-setting exercises to define specific large scale demonstration projects with high levels of EU added value in the second phase.

3.3.2 Requirements of different administrative elements for participants

In anticipation of participants stating that the programme's administrative requirements were unduly burdensome, respondents were asked to estimate the **share of their overall project input** that was spent on different administrative tasks. Respondents were invited to select one of four levels of input effort, ranging from the lowest level of 'no input (0%)' to an upper level of '6-10% of total project effort.'

[35] For the executive summary and the complete case study see Appendix E and Appendix F respectively.

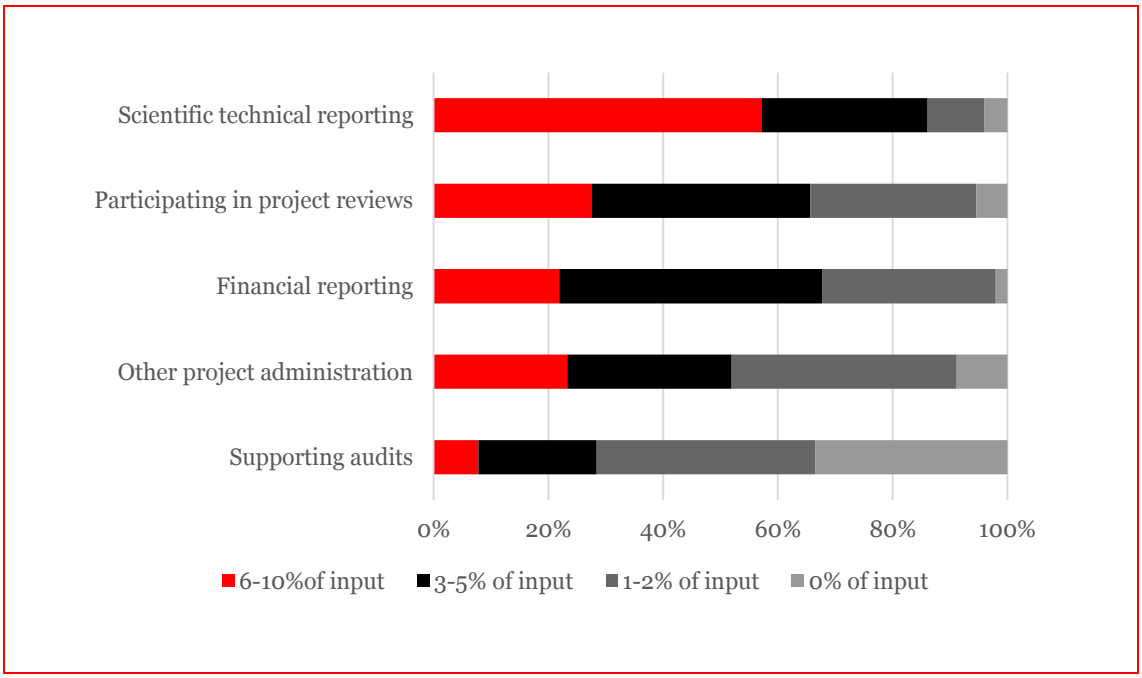
Figure 6 presents the results on overall project input for participants, while Figure 7 shows the results for project coordinators. Several findings emerge from analysis of these data:

- Scientific and technical reporting was most widely cited as being the most time-consuming administrative activity for participants, with almost 60% of respondents indicating that these responsibilities consumed 6-10% of their total project effort and more than 90% estimating that it consumed as much as 5% of their total project input. 'Support for audit' was the administrative cost item that was least widely cited as a major cost;
- More than 50% of respondents judged each of the other cost items to have consumed at least 3-5% of project effort;
- Project coordinators indicated that the administrative workload was more evenly distributed between technical reporting, financial and general administration. In all cases, more than 40% of responding coordinators estimated a workload of 6-10% of project activity overall. This suggests that perhaps 20-40% of a coordinator's total contribution is given over to administering projects;
- Both groups reported that supporting audits took up relatively little time.

The use of percentage range-bands secured a good response rate to the question, but does not allow a simple computation of average total administrative effort for the programme overall; however, based on the feedback obtained, the average 'burden' is unlikely to be less than 10% and **more likely to be in the range of 15-20% of total effort**. Working with the lower estimate of 10%, the results suggest that the cost to participants of administering their Security Research projects has an overall monetary value of perhaps €180m: that is around 10% of the €1.79b estimated value of total project activity supported by the FP7 Security Research Actions overall.

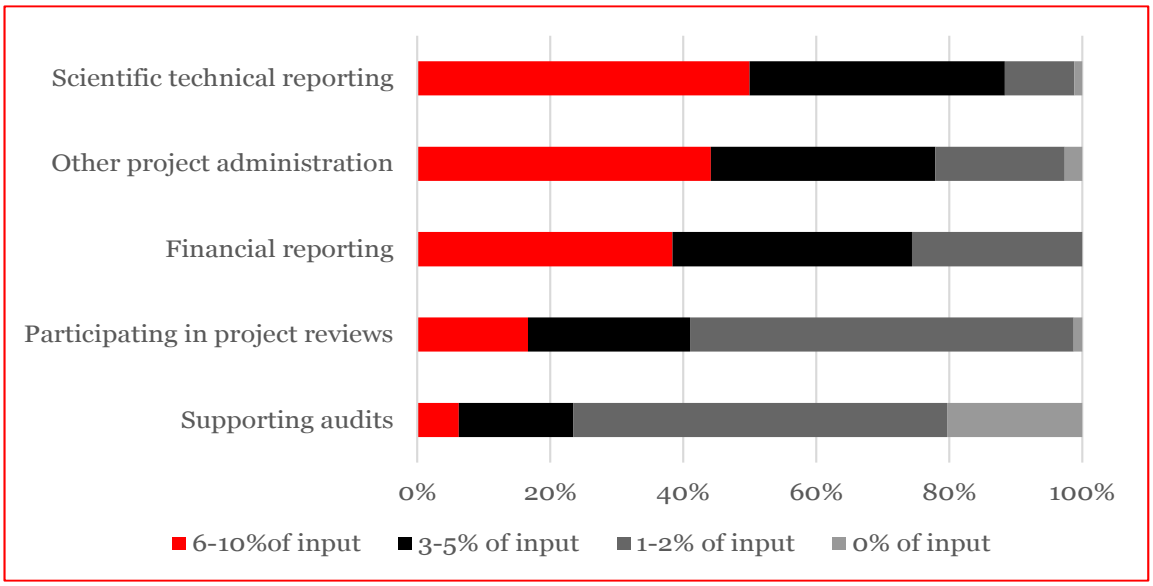
The analysis also confirms the expected **marked difference** between the overall administrative workload undertaken by project coordinators as a share of total project activity as compared with the administrative workload borne by other participants.

Figure 6: Estimate the share of your / your organisation's overall project input that was spent on the following administrative tasks (participants) (n = 573)



Source: Technopolis survey of FP7 Security Research participants, November 2014

Figure 7: Estimate the share of your / your organisation's overall project input that was spent on the following administrative tasks (coordinators) (n = 92)

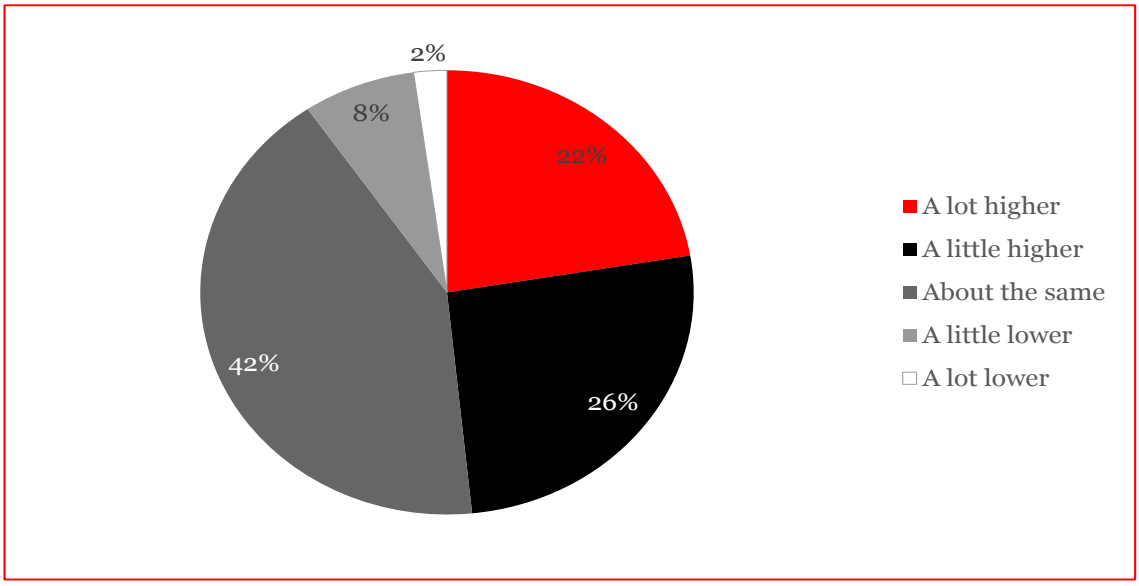


Source: Technopolis survey of FP7 Security Research participants, November 2014

Respondents were also asked to indicate how the FP7 Security Research Programme compares with other security research schemes, in terms of the weight of its administrative requirements.

The feedback (presented in the figure below) suggests that the FP7 Security Research Actions place **slightly greater administrative demands** on participants than do other security programmes: 49% of respondents believe that the administrative burden is higher compared with other programmes; while another 49% of respondents hold the view that the administrative burden is about the same or a little lower than other programmes, most of which are national rather than international in scope.

Figure 8: How does the FP7 Security Programme compare with other similar research programmes in terms of weight of administrative requirements? The requirements of the FP7 Security Research Programme are… (n=461)



Source: Technopolis survey of FP7 Security Research participants, November 2014

3.3.3 Impact of simplification measures within FP7

The Commission Services are aware of the administrative cost to applicants and participants, and have implemented simplification measures across successive EU framework programmes in an effort to improve the situation (to minimise social costs[36]). These measures are also designed to attract applications from a broader audience of smaller or less experienced organisations that may otherwise be dissuaded from applying by the administrative rules and associated costs.

The transition from FP6 to FP7 was accompanied by the implementation of a series of simplification measures and new online tools in an effort to streamline application processes and project administration.

The participant survey attempted to obtain feedback on the impact of these different measures, and respondents were asked to indicate to what extent a given simplification measure had indeed resulted in an improvement in the programme's administrative arrangements. Where respondents expressed a view, the balance of opinion was strongly positive, which coincides with an earlier assessment of the impact of the new measures across FP7.

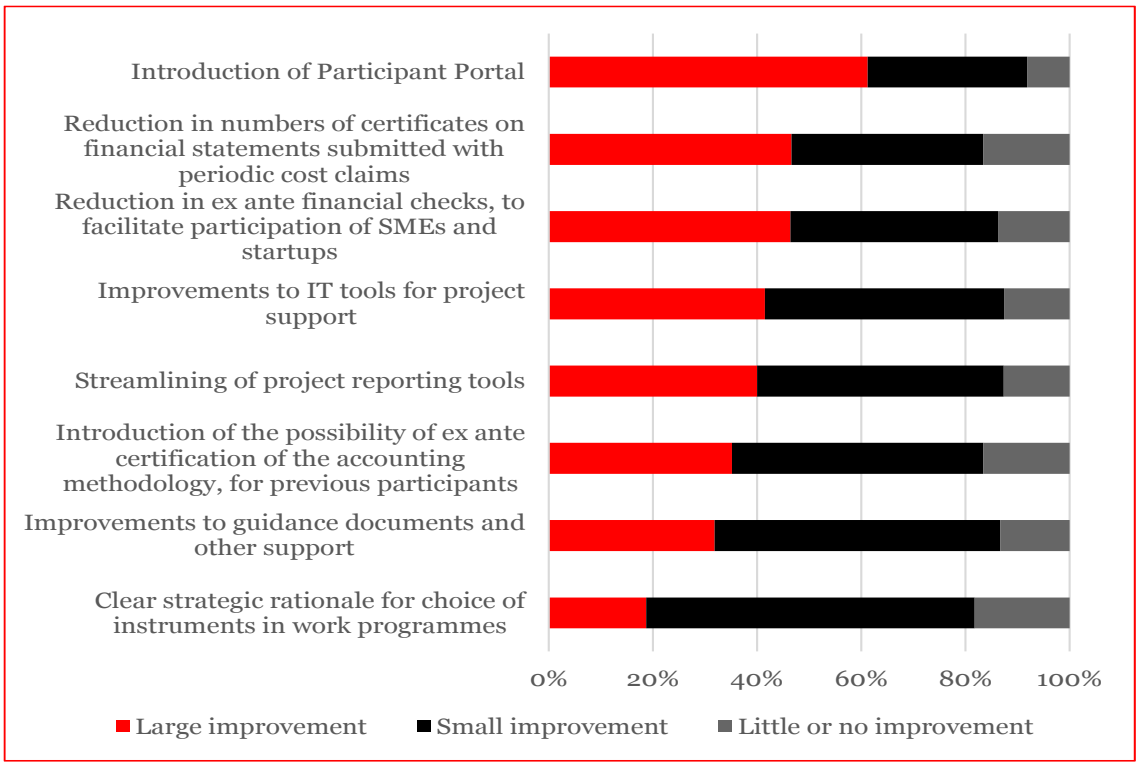
Around 60% of the respondents who answered the question on simplification indicated that they **"did not know"** what difference the various changes had made, which possibly reflects the fact that the individuals replying were the technical contact points of the projects rather than administrators and thus may have had less knowledge of the changes. It may also reflect the fact that Security Research was effectively new to FP7, so many respondents had little or no previous experience with EU RTD Framework Programme arrangements. Notwithstanding this possible blind spot, most respondents had strong views on the 'reasonableness' of FP7 administrative requirements more generally.

For the 30-40% of respondents who had a view on the impact of the various simplification measures, the introduction of the **Participants' Portal** is the development that is judged to have had a larger positive impact by the greatest share of respondents (60% of all participants and 75% of coordinators). There are several other differences in the responses of coordinators and participants concerning the changes that are most widely regarded as having been beneficial: a greater share of coordinators, for example, views the improved reporting tools as being a 'large benefit,' while for participants the big wins are the reduction in the numbers of certificates and *ex ante* financial checks.

End-users are generally more positive in their assessments, whereas a greater share of other participants tended to respond by stating that there had been "little or no improvement" as a result of the different changes.

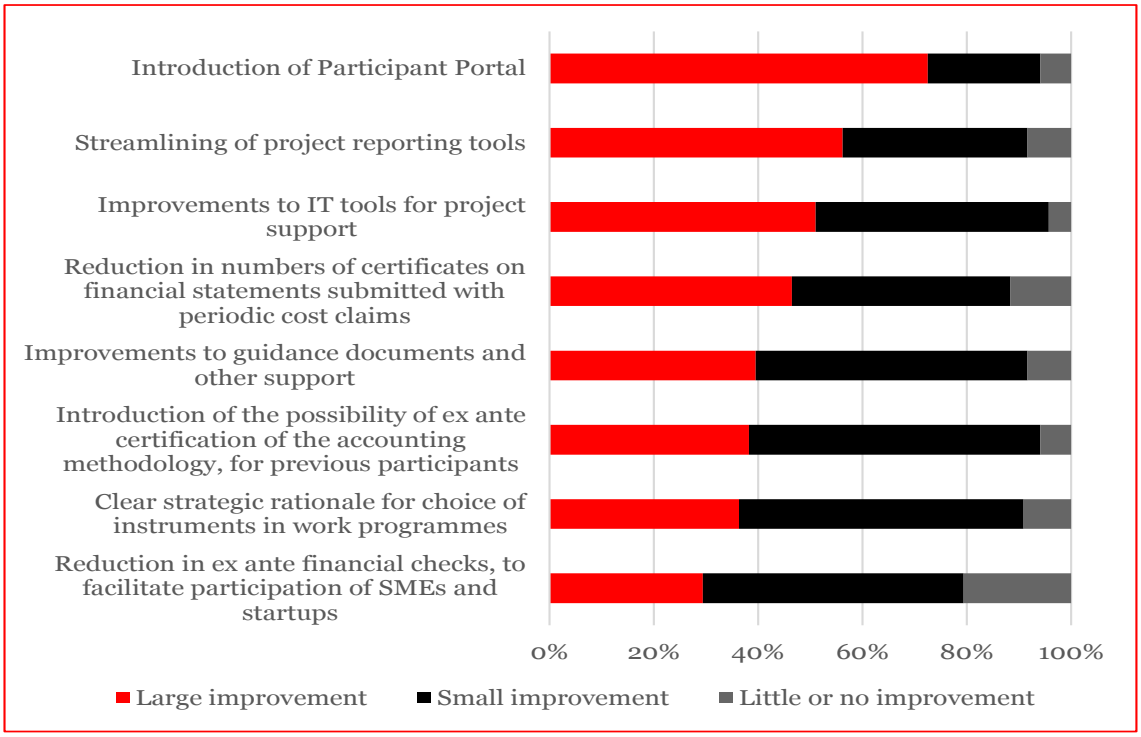
[36] The overall social cost also reflects the balance between the supply of public funds and the volume of demand for those grants or subsidies. All things being equal, a scheme that attracts 10 applications for every grant supported will be creating more social costs in the wider research system than a scheme that is able to fund one in five of its applications or one in three. In a worst-case scenario, where demand far outweighs supply, a support measure may conceivably cause more money to be spent on preparing applications than it awards in grants. Applying is not a zero-sum game though: the competition among contractors and beneficiaries is believed to improve the quality of project proposals and consortia and thereby enable public schemes to deliver more social benefit from a given investment. Equally, the preparation of an unsuccessful proposal can lead applicants to proceed with that work independently or through an alternative funding route; proposals are rarely discarded, and most will be submitted to subsequent calls having been updated or otherwise strengthened in line with feedback from previous evaluation rounds.

Figure 9: To what extent have the simplification measures that were introduced with the launch of FP7 resulted in improvements? (Participants) (n = 573)



Source: Technopolis survey of FP7 Security Research participants, November 2014

Figure 10: To what extent have the simplification measures that were introduced with the launch of FP7 resulted in improvements? (coordinators) (n = 92)



Source: Technopolis survey of FP7 Security Research participants, November 2014

Many of the concerns expressed about FP7's **administrative burden and procedural inefficiencies** have been addressed, in part at least, in the progression from FP7 to Horizon 2020, and therefore will not form part of the recommendations here. Those important simplification measures are spelled out in a short document entitled 'fact sheet on rules under Horizon 2020.'[37] The following list provides a selection of changes that will both simplify matters for applicants and shift the point of balance between trust and control towards trust:

- A single set of participation rules (covering issues such as eligibility, evaluation, Intellectual Property Rights, etc.) applying to all components of Horizon 2020;
- Electronic signature of grants and amendments to simplify and speed up administrative procedures;
- Simpler reimbursement of direct costs, with a broader acceptance of the beneficiaries' usual accounting practices;
- The possibility of using unit personnel costs (average personnel costs) in accordance with the beneficiaries´ usual cost accounting practices;
- Abolition of time-recording obligations for staff working exclusively on an EU project, and simplification of time-recording requirements for other staff by providing a clear and basic set of minimum conditions;
- Indirect costs covered by a single, flat-rate applied to the direct costs, removing a major source of financial errors and complexity.

3.3.4 Efficient promotion

An analysis of demand for FP7 Security funding (based on a comparison of eligible and retained proposals) was provided in Section 3.2. This suggested a relatively high 'excess-demand' on the Security Programme compared with most other areas of the wider Cooperation Programme, with six proposals submitted (three above the minimum quality threshold) and €5.2 requested for every proposal retained and €1 contributed by the EC, respectively. This suggested that **the programme was well promoted**, and was able to attract greater interest (of a high quality) than it was able to fund.

However, while it may be desirable to have a larger number of proposals from which to select a smaller number of projects to fund, the lower success rate in comparison with most other parts of the Cooperation Programme suggests there may be some degree of wasted effort over and above the minimum required to secure a portfolio of high quality projects. Data on the distribution of proposals by mission area and funding instrument are not available, and so it is not possible to consider demand and supply by these variables.

[37] European Commission (2010) Factsheet: Rules under Horizon 2020. Brussels: European Commission.

3.4 Evidence Building Block 3: Direct Achievements ("what")

3.4.1 Attracting the 'best and brightest'

EQ14. Did the research activity attract the EU's best researchers or leading research organisations? Did the instruments reach the appropriate communities? What was the take-up for different types of actors – academia, enterprises, SMEs etc.?
Key indicators: Number of articles published in high impact journals; number of articles per €10m EC contribution; list of top 10 journals by impact factor; Distribution of participations by types of actors (applications and grants) for the programme overall and main mission areas; Top 50 participants

FP7 Security Research is committed to supporting applied research of the highest quality, and in order to achieve that goal, it sought to attract high-quality applications from strong project consortia including most of the EU's major security research groups.

Security research is a relatively new policy **concept**, which brings together very many different areas of applied science and technology, from electronics to applied healthcare, from mathematics to sociology. It is still rather heterogeneous, and as such many interviewees found it hard to say whether the programme has attracted the best and the brightest academic research groups. Interviewees were rather more confident about the programme's successful engagement of leading national research laboratories and major defence and security companies. These are small in number and well known. Interviewees believe that the most active organisations have all been involved in the programme, a view they came to through attendance at events and the more general monitoring of the programme's project listings and calls.

The desk research confirms this view. While there is no **single list cataloguing Europe's leading security research organisations**, a rapid reading of the top 50 participants reveals a 'Who's Who' of notable organisations with a longstanding interest in security-related research across the public and the private sectors. The list includes:

- Specialist national laboratories, like the Swedish Defence Research Agency (FOI);
- Leading security think tanks, like Demokritos;
- Major defence and security manufacturers, like Finmeccanica;
- University research groups with a particular interest in security issues;
- International security agencies, like INTERPOL or EUROPOL;
- Home Affairs ministries, like Spain's Ministry of the Interior.

The top 50 participants include a high proportion of large public research institutes with a very much wider research remit than simply security, including the Fraunhofer institutions (a German research organisation with 67 institutes and Europe's largest applied research organisation), TNO (the Netherlands Institute for Applied Scientific Research) and VTT (the Technical Research Centre of Finland). The breadth of interests of these leading national research institutes is confirmed by the fact that 20 of the top 50 Security Research organisations are also listed in the top 50 participants for the FP7 Cooperation Programme overall.

The analysis shows that Europe's leading security research organisations are participating in FP7 Security Research projects. The top three organisations (as per total EC funding) are Fraunhofer, FOI (Swedish Defence Research Agency), and TNO (Netherlands Organisation for Applied Scientific Research), directly followed by THALES, a major multinational company.

The first higher education establishment to appear in the top 50 is the University of Leuven in Belgium.

3.4.2 Volume and quality of research publications

The Security Research Programme has produced relatively **few research publications**, reflecting its focus on capability building and demonstration activities. One would expect this rather operational focus to result in a relatively low number of publications compared with other parts of the FP7 Cooperation Programme.

SESAM data show that 41% of the projects assessed so far (25 of 61) resulted in at least one publication (paper/article) over and above the contract research report, and that together these projects reported **214 publications in total**. This is a partial dataset, comprising only projects from the earliest calls and those of shorter duration, and so the total number of publications will eventually be substantially higher. Nevertheless, so far this equates to 3.5 publications for every project assessed (if all projects are included, regardless of whether they produced a publication or not), or 8.6 publications per project (if only those are included that report at least one publication). The projects assessed to date have a combined EC contribution of €147.1m, and so there are 15 publications reported for every €10m of EC contributions.

Table 22: Projects producing publications (n=61)

Mission	Projects assessed	At least 1 publication	Total pub's	Pubs per project assessed	Pubs per €10m EC contribution
Security of citizens	10	60%	42	4.2	17
Security of infrastructures and utilities	7	43%	10	1.4	5
Intelligent surveillance and border security	4	50%	3	0.8	1
Restoring security and safety in the case of crisis	11	45%	32	2.9	10
Security and society	11	55%	63	5.7	34
Security Research coordination and structuring	10	0%	0	0.0	0
Security systems integration, interconnectivity and interoperability	8	38%	64	8.0	34
Total	**61**	**41%**	**214**	**3.5***	**15***

Source: Technopolis analysis of SESAM Monitoring Data, October 2014. *Average for all projects

As can be seen in Table 22, there are **differences between the publication profiles of projects** in each of the seven mission areas, and compared with the aggregate picture (see bottom row). For example, the share of projects producing at least one publication varies between 0% and 60%, while the number of publications per project varies from none to eight, and the number of publications per €10m EC contribution from none to 34.

The 'security research coordination and structuring' mission area is consistently below average across each measure, while 'increasing the security of citizens' and 'security and society' are consistently above average. This variance has less to do with the 'productivity' of the individual project teams and rather more to do with the types of actors and projects one finds in the different mission areas: security of citizens, for example, has a disproportionate share of academic participations, which will tend to publish more papers and journal articles on average; while the research coordination mission includes more public authorities and coordination actions, which will tend to publish fewer articles on average.

Of the 214 publications reported overall, 34 (16%) were published in **high-impact**[38] peer-reviewed journals. This equates to 0.6 such publications per project assessed, or 1.4 such publications per publishing project. There were 2.3 publications in high-impact peer-reviewed journals for every €10m of EC contributions.

[38] High-impact journals are defined to be the top 10% (in terms of SJR index) of all journals within a given scientific category. The SJR index is a Journal Rank Indicator and measures a journal's impact, influence or prestige. It expresses the average number of weighted citations received in the selected year by the documents published in the journal in the three previous years (2011).

Table 23 compares SESAM-derived publication figures for Security Research (as of the end of December 2014) with the same statistics for several other parts of the Cooperation Programme, which were compiled several months earlier (October 2014) as part of the ex post evaluation of the FP7 Space Research Actions. The table shows that the Cooperation Programme overall has a very much stronger performance on this indicator, as compared with the Security Research Programme, with an average of more than 12 publications per project of which more than six are publications in high-impact journals. Again, this is a reflection of the type of research being carried out in other Thematic Areas, as well as the larger average size of projects in several areas; health, for example, has ratios of around 24 publications per project of which 11 are publications in high-impact journals.

Table 23: Number of publications per project for key comparators

Priority area	Projects with a final report	Number of publications	Publications in high-impact peer-reviewed journals	%	Average publications per project
Transport	98	78	21	27%	0.8
Security	61	214	34	16%	3.5
Space	101	565	204	36%	5.6
NMP	119	1,466	763	52%	12.3
All Cooperation Prog.	731	9,060	4,536	50%	12.4

Source: Technopolis analysis of SESAM Monitoring Data, October 2014

3.4.3 Distribution of participation and EC financial contributions

EQ15. Were there gaps or uneven distribution in terms of e.g. thematic areas, gender, and geographical coverage?

Key indicator: Distribution of participations by geography; Distribution of participations and EC contributions for the programme and mission areas, by gender

3.4.3.1 Participations and funding by mission areas

As already noted, the distribution of participations and EC contributions across the mission areas of the Security Programme was **not even**. Three of the main security missions in particular accounted for an above-average share of Security projects, participations and EC contributions: these were the 'security of citizens'; 'security of infrastructures and utilities'; and 'restoring security and safety in case of crisis' mission areas. The three cross-cutting missions accounted for just 23% of EC contributions to the Security Programme, while the four main mission areas accounted for the other three quarters.

From the team's reading of the situation and feedback from participants and stakeholder interviews, this 'uneven' distribution does not constitute an imbalance in the portfolio and there are no fundamental gaps in the programme's coverage.

3.4.3.2 Participation and funding by geography

There were **48 different countries** involved in FP7 Security projects (on average 78 participations per country). The average project, with 12 participants, included participating organisations from 7 different countries.

The table below lists each participating country (and the EU through the JRC), and provides details on the number of projects, participations and total EC contributions to each. The table is sorted in descending order of EC contributions, and shows Germany, the UK, France, Italy and Spain to be the 'top' participants in the programme (each with €100m+ in EC contributions and 300+ participations). The top non-EU Member States appearing in the list are Norway and Israel (13th and 14th).

Table 24: Projects, participations and EC contributions, by country[39]

Country	Code	EC contribution	Participations (and rank[40])	Projects
Germany	DE	€159,862,017	380 (3)	199
United Kingdom	UK	€152,305,365	430 (1)	210
France	FR	€151,541,607	379 (4)	172
Italy	IT	€121,772,196	385 (2)	173
Spain	ES	€110,920,970	319 (5)	157
Netherlands	NL	€79,123,262	240 (6)	131
Sweden	SE	€62,294,867	144 (9)	103
Belgium	BE	€52,099,167	168 (7)	112
Austria	AT	€44,060,629	123 (10)	78
Greece	EL	€43,776,916	150 (8)	76
Poland	PL	€33,178,421	102 (11)	75
Finland	FI	€31,869,588	97 (12)	66
Norway	NO	€31,615,361	84 (14)	65
Israel	IL	€31,523,521	85 (13)	56
Switzerland	CH	€28,543,070	80 (16)	59
Ireland	IE	€26,075,799	79 (17)	58
Portugal	PT	€21,651,038	84 (14)	55
Denmark	DK	€14,257,242	41 (18)	33
Slovakia	SK	€7,125,091	25 (24)	19
EU (JRC)	EU	€6,759,664	26 (23)	26
Czech Republic	CZ	€5,789,696	34 (20)	32
Turkey	TR	€5,209,062	28 (21)	25
Luxembourg	LU	€5,033,438	19 (28)	15
Slovenia	SI	€4,457,149	25 (24)	23
Romania	RO	€4,351,272	38 (19)	35
Cyprus	CY	€4,162,720	15 (29)	14
Estonia	EE	€3,686,642	21 (26)	17
United States	US	€3,587,938	11 (33)	8
Hungary	HU	€3,536,682	27 (22)	24
Croatia	HR	€3,497,820	13 (31)	8
Bulgaria	BG	€2,321,091	21 (26)	21
Latvia	LV	€1,542,817	14 (30)	12
Lithuania	LT	€1,204,977	12 (32)	11
Malta	MT	€1,114,228	9 (34)	9
Serbia	RS	€1,039,840	5 (35)	5
Japan	JP	€646,242	4 (36)	4
Iceland	IS	€553,035	3 (38)	2
Australia	AU	€375,996	2 (39)	2
Ukraine	UA	€263,280	2 (39)	1
Russia	RU	€175,950	1 (45)	1
Bosnia-Herzegovina	BA	€153,548	1 (45)	1
FYROM	MK	€118,125	2 (39)	2
India	IN	€115,490	2 (39)	2
Egypt	EG	€56,800	1 (45)	1
South Africa	ZA	€54,947	2 (39)	2
Canada	CA	€35,614	4 (36)	4
Palestine	PS	€25,231	1 (45)	1
Montenegro	ME	€22,622	1 (45)	1
Taiwan	TW	€ -	2 (39)	1
All		**€1,263,488,044**	**3,741**	**307**

Source: Technopolis analysis of CORDA data

The following table shows the **top 50 participants by number of participations** in the Security Research Programme per million population of the country of origin. Utilising this measure, the top participating countries in the Security Programme (relative to population) are Luxembourg, Malta, Finland, Cyprus, Ireland, Norway, Estonia, Sweden and Belgium.

[39] In the table, each country with 100 or more participations is shaded grey.

[40] The number in brackets indicates the rank of the country if the data is sorted according to the number of participations.

The final column shows the **share of each country's overall number of participations** in the Cooperation Programme that are accounted for by their participations in the Security Programme. According to this measure, the top participating countries are Luxembourg, Malta, the Palestinian administered areas, Israel, Slovakia and Latvia (as well as the JRC), each with at least 8% of their Cooperation Programme participations accounted for by the Security Programme (and therefore double the rate of SEC-to-Cooperation participation overall).

Table 25: Geographical participations per million population[41]

Country	Code	Participations	Participations per m pop.	SEC as % of Cooperation participations
Luxembourg	LU	19	35.4	11.0%
Malta	MT	9	21.4	10.5%
Finland	FI	97	17.9	5.2%
Cyprus	CY	15	17.3	6.7%
Ireland	IE	79	17.2	6.6%
Norway	NO	84	16.3	6.0%
Estonia	EE	21	15.9	7.6%
Belgium	BE	168	15.1	4.3%
Sweden	SE	144	15.1	4.7%
Austria	AT	123	14.6	4.9%
Netherlands	NL	240	14.3	4.3%
Greece	EL	150	13.6	6.1%
Slovenia	SI	25	12.1	4.1%
Israel	IL	85	10.3	9.1%
Switzerland	CH	80	9.8	2.8%
Iceland	IS	3	9.1	1.9%
Portugal	PT	84	8.0	5.7%
Denmark	DK	41	7.3	2.3%
Latvia	LV	14	6.9	8.4%
Spain	ES	319	6.8	4.6%
United Kingdom	UK	430	6.7	4.4%
Italy	IT	385	6.5	4.6%
France	FR	379	5.8	4.5%
Germany	DE	380	4.7	3.0%
Slovakia	SK	25	4.6	8.9%
Lithuania	LT	12	4.0	5.6%
Czech Republic	CZ	34	3.2	3.9%
Croatia	HR	13	3.1	5.8%
Bulgaria	BG	21	2.9	5.7%
Hungary	HU	27	2.7	3.2%
Poland	PL	102	2.6	7.6%
Romania	RO	38	1.9	5.9%
Montenegro	ME	1	1.6	7.1%
FYROM	MK	2	1.0	4.1%
Serbia	RS	5	0.7	2.9%
Turkey	TR	28	0.3	5.4%
Bosnia-Herzegov.	BA	1	0.3	4.8%
Palestine	PS	1	0.2	9.1%
Canada	CA	4	0.1	2.4%
Australia	AU	2	0.1	1.3%
Taiwan	TW	2	0.1	7.1%
United States	US	11	0.0	2.5%
Japan	JP	4	0.0	4.7%
Ukraine	UA	2	0.0	1.5%
India	IN	2	0.0	1.0%
South Africa	ZA	2	0.0	1.0%
Russia	RU	1	0.0	0.2%
Egypt	EG	1	0.0	1.2%
EU (JRC)	EU	26	n/a	9.2%
All		3,741		4.3%

Source: Technopolis analysis of CORDA data

[41] In the following table each country with 15 or more participations per million population is shaded.

It is worth noting that there were participations from 118 other countries in the wider Cooperation Programme, but not in the Security Research Programme. This includes eight countries (listed below) that have over 50 participations in other parts of the Cooperation Programme. The final column shows the number of participations from these countries that one might expect to see in the Security Programme based on their overall (Cooperation Programme) participation level, and the fact that Security accounts for around 4% of Cooperation Programme participations overall.

Table 26: Major participants in the Cooperation Programme (not SEC)

Country	Code	Participations in the Cooperation Programme	'Expected' SEC participations
China	CN	303	12
Brazil	BR	192	8
Mexico	MX	102	4
Morocco	MA	96	4
Argentina	AR	92	4
Tunisia	TN	68	3
Kenya	KE	63	3
Chile	CL	53	2

Source: Technopolis analysis of CORDA data

3.4.3.3 Participation by gender

There are several sources of data on the gender of those involved in Security Programme participations, none of which is entirely comprehensive.

Where known (96% of participations), the majority (83%) of **lead scientific contact points** for participations in FP7 Security projects were male, while just 17% were female. This rate was similar across all seven of the mission areas.

Separate data held on a selection of **key personnel** for 306 Security projects provides further information on the gender of some of the other individuals involved in participations (see below). Again, men outnumber women at a rate of around 4 to 1.

Table 27: Gender distribution of key project personnel

	Male	Total personnel listed
Contact Person	68%	3,722
Contact Person for Scientific Aspects	83%	3,617
First Administrative Officer	89%	3,687
Secondary Administrative Officer	80%	2,365
Total	80%	13,391

Source: Technopolis analysis of CORDA data

All 61 Security projects that have submitted a final report that has been processed within the SESAM database have also encoded a **workforce report**. These reports show a combined workforce of 3,506 people – or 57 per project on average. Overall, the majority of this workforce (69%) was male and 31% female. This rate is similar across all mission areas and all workforce categories (with the exception of PhD students in the 'security and society' area), as can be seen below.

Table 28: Share of workforce that is male

Mission Area	Scientific managers	Experienced researcher (i.e. PhD holders)	PhD student	Work package leaders	Other	Total workforce
Security of citizens	86%	58%	64%	84%	70%	68%
Security of infrastructures and utilities	86%	85%	80%	87%	78%	81%
Intelligent surveillance and border security	71%	88%	77%	88%	71%	77%
Security and safety in case of crisis	92%	66%	56%	78%	60%	64%
Security and society	53%	61%	46%	69%	55%	57%
Security Research coordination and structuring	63%	64%	63%	67%	52%	61%
Security systems integration, interconnectivity and Interoperability	79%	79%	82%	74%	72%	76%
Total	75%	70%	62%	78%	66%	69%

Source: Technopolis analysis of CORDA data

3.4.3.4 Industry / SME participation – impacts on the security industry

The programme achieved a high level of engagement with Europe's security industry. Nearly all (93%) of the FP7 Security **projects** involved at least one Private Commercial participant (i.e. industry), with nearly as many involving at least one PRC-SME (86%). In the individual mission areas, the rate of PRC involvement varied between 83% and 100% of projects. This is well above the rate for the Cooperation Programme overall (83%), and higher than most other thematic areas with the exception of NMP (94%), Energy (95%) and Transport (95%).

As already mentioned, 43% of all **participations** in the Security Programme were from PRCs – higher than any other organisation type – with nearly half (49%) of these being SMEs (which accounted for 21% of all participations). The rate of participation from PRC organisations was only substantially lower in two mission areas: 'security and society' (24%) and 'security research coordination and structuring' (28%). PRC participation in the Security Research Programme is considerably higher than for the Cooperation Programme overall (35% of all participations).

Industry received about €580m in **EC contributions**, accounting for almost half of the total for the Security Research Programme. Nearly half (€263m) of this figure went to SMEs. The average contribution to PRCs (€364k per participation) is above average for the Security Research Programme overall (for all types of participant), and also 23% higher than the average contribution to PRCs across the Cooperation Programme as a whole.

CORDA data show the Security Research Actions **comfortably exceeded the target for SME participation** set by the Commission for the Cooperation Programme overall, with SMEs accounting for 21% (785) of all security participations and 21% (€263m) of total EC contributions. The figure for FP7 overall is 19%.

The discussion at the focus group (stakeholder) workshop **challenged this positive outlook**, arguing that the SMEs in question were predominantly private technology centres or consultancies specialised in the management of FP7 projects. Several focus group delegates claimed that the Security Research Programme has been rather less successful at attracting and supporting proposals from smaller technology firms with the capacity to transform the newly developed know how and relationships into jobs and growth. Cross-checking the web sites of the most active SMEs (e.g. top 20 SMEs by number of participations), confirms that these are mostly technology centres developing capabilities that they will subsequently sell to other businesses, including SMEs. Clearly, these kinds of intermediaries have an important role to play in an innovation ecosystem, and it is perhaps not surprising that the most active SME participants are service businesses, while the high-tech manufacturers tend to be involved in single projects, reflecting their sharper focus on IP for proprietary business development.[42]

Several other workshop participants concurred and remarked that FP7, with its long project duration and large partnerships, is **not best suited for high-tech SMEs** even though many of the topics are of interest. One participant also mentioned that according to his observations, many SMEs participating in projects were performing management and dissemination tasks. On a separate but related point, delegates also mentioned an issue involving confidentiality and research results, as SMEs and end-users have experienced difficulties in getting access to results. These concerns did not figure in the feedback from SMEs responding to the participant survey, where the biggest concern, after project success rates and time-to-grant, was the absence of any meaningful follow-on support to help with commercialisation beyond the life of the FP7 project. This may reflect an unobserved response bias, with the SME respondents possibly being dominated by the more active and more experienced technical consultancies.

[42] This phenomenon is not unique to Security. According to the 7th Monitoring Report for FP7, there is not a single high-tech SME manufacturer in the top 25 SMEs, for FP7 overall, with Ateknea Solutions (a private, product development company in Barcelona), placed first on number of participations (66 participations) and the DANTE network of national academic research infrastructures (GEANT) in Cambridge placing first on income (€84m).

The evaluation team were not able to effectively address the underlying concern expressed that SME consultancies may be crowding out technology SMEs from pursuing better growth prospects, as this was not a line of enquiry that was followed in the interviews or surveys. It does however constitute a legitimate issue, which would benefit from **further research**. It is also possible that such displacement, if it is happening, would tend to affect disproportionately those Member States with a good base of technology SMEs, but with little or no established security or defence industries.

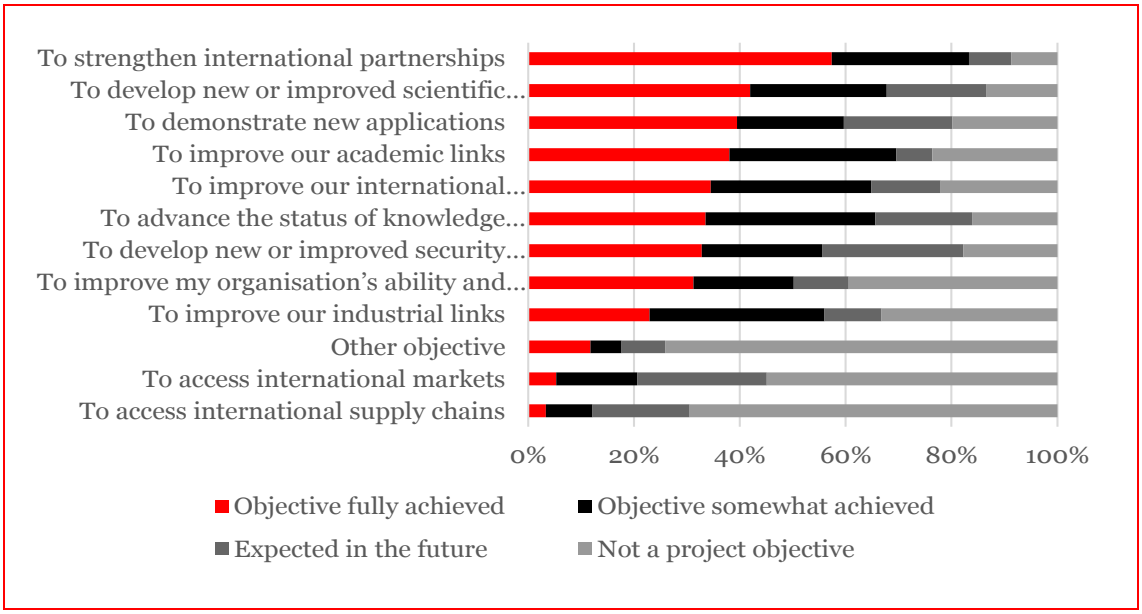
3.4.4 Project-level achievements

3.4.4.1 Project objectives and their achievement

Project coordinators were invited to select from a menu of potential project objectives to indicate the specific focus of their project, and to judge the extent to which those objectives had been achieved, or are likely to be achieved in the future.

Figure 11 presents the results – sorted by the share of respondents who report that the objective in question has been achieved in full. Stronger international partnerships is the most widely cited achievement, with "accessing international markets" or "supply chains" having been achieved fully by fewer than 10% of respondents for whom that was a project objective.

Figure 11: Which of the following elements were objectives of the project, and to what extent have they been achieved (or are likely to be achieved)? (project coordinators) (n = 599)



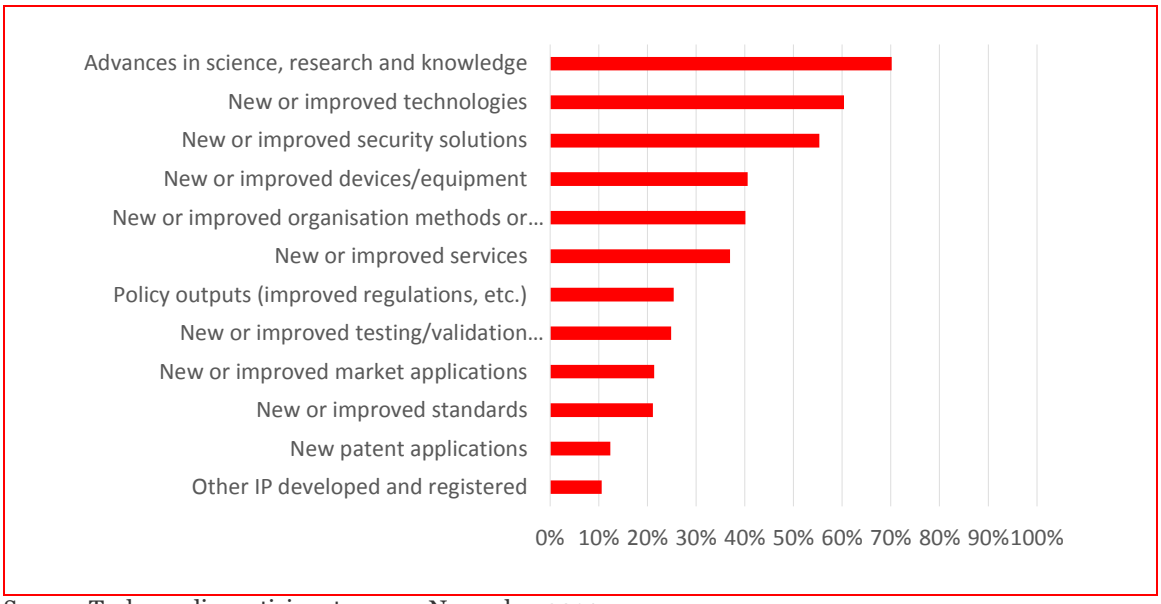
Source: Technopolis participant survey, November 2014

3.4.4.2 Project results

The participant survey invited respondents to use a menu of anticipated 'standard' project results to indicate which specific results they had realised through their participation in a given FP7 Security Research project. The figure below shows the share of all respondents that has realised or expects to realise a given type of project result, sorted by share of responses (in descending order).

Advances in knowledge, new or improved technologies and improved security solutions are the three results that were most widely reported. Around 20% of respondents have seen or expect to see their project result in policy outputs, market applications and standards, and new patents.

Figure 12: Indicate whether any of the following have resulted (or are expected to result) from the FP7 projects (n = 611)



Source: Technopolis participant survey, November 2014

The respondents also had the opportunity to list any other types of output that have resulted (or are expected to result) from their project participation, in order to avoid the risk that the pre-defined menu has overlooked important categories of results. Common responses were:

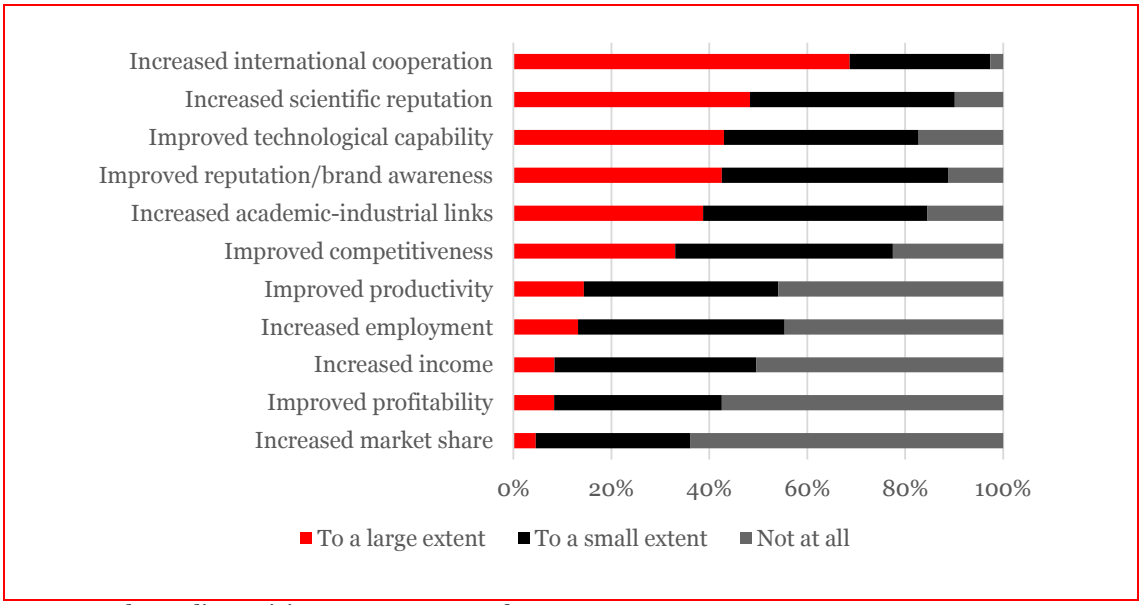
- Publications;
- New methodologies and tools;
- New partnerships and collaborations;
- Improved cooperation and partnerships (public/private);
- New networks and business opportunities;
- New business models;
- New training methods, university courses;

3.4.4.3 Impact on participating organisations.

Moving on from considerations regarding project results, the survey respondents were asked to indicate what if any impact their participation in the Security Research Programme had had on their organisation overall.

The figure below shows that the most widely reported **'larger effect'** was on the organisation's international relationships and cooperation (70%). Other widely reported impacts include improvements to reputation, capability and industry-academic links. Perhaps unsurprisingly, only a small share of respondents stated that their participation(s) had had a positive impact on the overall performance of their organisation in terms of employment, income or profitability. These aspects are really only of relevance to businesses, of course, which constitute around 50% of the individual organisations participating in the Security Research Programme.

Figure 13: To what extent do you believe participation in the project had the following positive impacts on your organisations (n = 594)



Source: Technopolis participant survey, November 2014

The respondents were also given the opportunity to describe any other types of important organisational **benefits**. Examples of other benefits mentioned were:

- Cooperation (national, cross-disciplinary, with companies and institutes), alignment with organisations, new networks;
- Exchange of experiences within the EU;
- New products and services;
- Scientific publications;
- Achieved commercialisation, spin-off company;
- Feedback from companies during development of prototype regarding usability;
- Ideas for product enhancements and new services;
- Experience in project management;

3.4.4.4 Project outputs and outcomes – research commercialisation.

Based on the analysis of SESAM data, 18% of the 61 completed Security Research projects that have been assessed were found to have 'good innovation potential', while 8% were completed with 'substantial R&D breakthrough character' and 5% with 'outstanding use / exploitation of results' (categories that are not mutually exclusive).

SESAM data also provided information on the generation of **intellectual property rights** (IPR)[43] within the projects that have been assessed (n=61). There are seven projects (11%) – spread across five mission areas – that have reported at least one IPR. Between them, these projects reported a total of 19 intellectual property rights, including 10 reported as a **patent application**. This is the equivalent of one IPR reported for every €7.7m of EC contributions (for the full set of 61 projects), and one patent application for every €16.3m of EC contributions. Looked at in another way, for every €10m of EC contributions to the 61 projects, 1.3 IPRs have been reported, including 0.6 patent applications.

[43] Defined here as legal rights aimed at protecting the creation of intellect, such as inventions, appearance of products, literary artistic and scientific works and signs, among others.

SESAM data also provide information on the production of other '**foregrounds'**. These are tangible and intangible results, including for example information and knowledge, whether or not it can be protected, which is generated under the project.[44] There are 10 projects (16% of the 61 assessed) that have reported the generation of at least one foreground. Most of these projects (7) fall within the 'security and society' and 'security research coordination and structuring' mission areas. Between them, the projects have generated 22 foregrounds of different types. This equates to 2.2 foregrounds per project generating a foreground, and 0.4 foregrounds for every project assessed. The generation of different types of foreground was as follows:

- Commercial exploitation of R&D results (9 of 61 projects);
- Exploitation of results through (social) innovation (5);
- Exploitation of results through EU policies (3);
- General advancement of knowledge (1);
- Exploitation of R&D results via standards (0).

Overall, for every €10m of EC contributions, projects have resulted in 1.5 foregrounds.

SESAM provides information on activities to **disseminate** the foregrounds produced (beyond any disclosure required as part of protecting that foreground).[45] Nearly all projects (90%) undertook at least one such dissemination activity, with 2,398 dissemination activities defined in total across the final reports of these projects. This equates to 44 dissemination activities per project undertaking dissemination, and 39 dissemination activities for every project assessed. For every €10m of EC contributions, 163 dissemination activities are recorded.

Dissemination activities included:

- 573 Presentations
- 511 Conferences
- 260 Publications
- 227 Workshops
- 176 Press releases
- 143 Web sites
- 84 Posters
- 71 Conferences organised
- 60 Flyers
- 53 Interviews
- 51 Exhibitions
- 44 Oral presentations at scientific events
- 39 Workshops organised
- 24 Oral presentations to a wider public
- 20 TV clips
- 20 Videos
- 19 Media briefings
- 18 Thesis
- 5 Films

As seen in the previous section, three projects (5%) were found to have achieved 'exploitation of results through **EU policies**', while in Section 3.2.3.3 it was shown that 14 projects (23% of those completed and assessed) were found to have had 'an impact on EU policies.'

The **focus group discussion was critical** of dissemination and exploitation efforts, arguing that project coordinators – and particularly those in the big research institutes – were too often concerned with the next research project and placed insufficient weight on the valorisation of the results of the current project. There was a general desire to see the programme do more about exploitation, rather than leaving it primarily to individual projects. Numerous suggestions were offered for improving dissemination, ranging from programme conferences to better information portals and repositories. The main recommendations related to exploitation (rather than dissemination) and the need for stronger incentives / requirements for projects to develop commercialisation plans along the way (and to be tested on these at the application stage) and for the Commission to find ways to provide follow-on funding to help firms take their ideas and technologies forward to the next stage.

44 Such results include rights to related copyright, design rights, patent rights, and similar forms of protection.

45 Note that while this is how SESAM defines dissemination activity, the number of projects involved far exceeds the number reporting a recognised foreground.

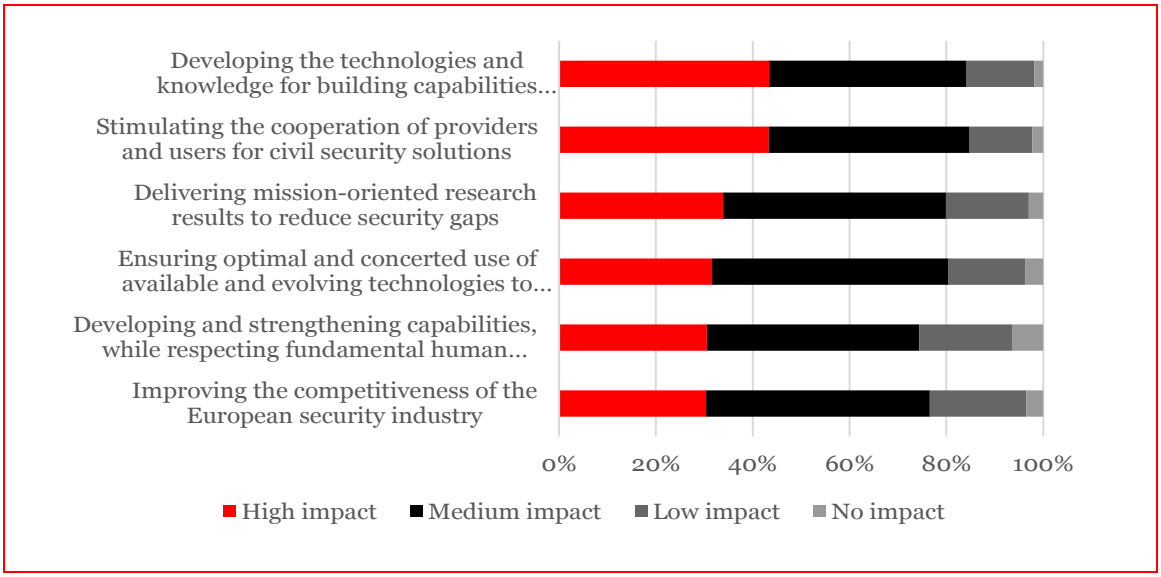
3.5 Evidence Building Block 4: Wider Achievements ("what")

3.5.1 Impacts of the programme on its specific objectives

Figure 14 shows that the great majority of participants (75%+) believe that the Security Research Programme has had a **high or medium impact on each of its specific objectives**. Judging programme impact is not easy for participants whose experience may be limited to an individual project or Work Programme, and only around 30% of respondents felt confident enough to express a view on this question.

There is very little difference in the feedback, objective by objective. On balance, a greater share of participants believed that the programme has made a substantial contribution to its 'developing technology to build capability' objective (85%) and a slightly smaller proportion (75%) felt it is making a positive contribution to strengthening the competitiveness of the EU security industry. None of the specific objectives set out in the Council Decision (COM 2006 364) was judged to have been overlooked.

Figure 14: What has been the impact of the FP7 Security Research Programme overall in relation to each of the following programme objectives? (n = 269)



Source: Technopolis participant survey, November 2014

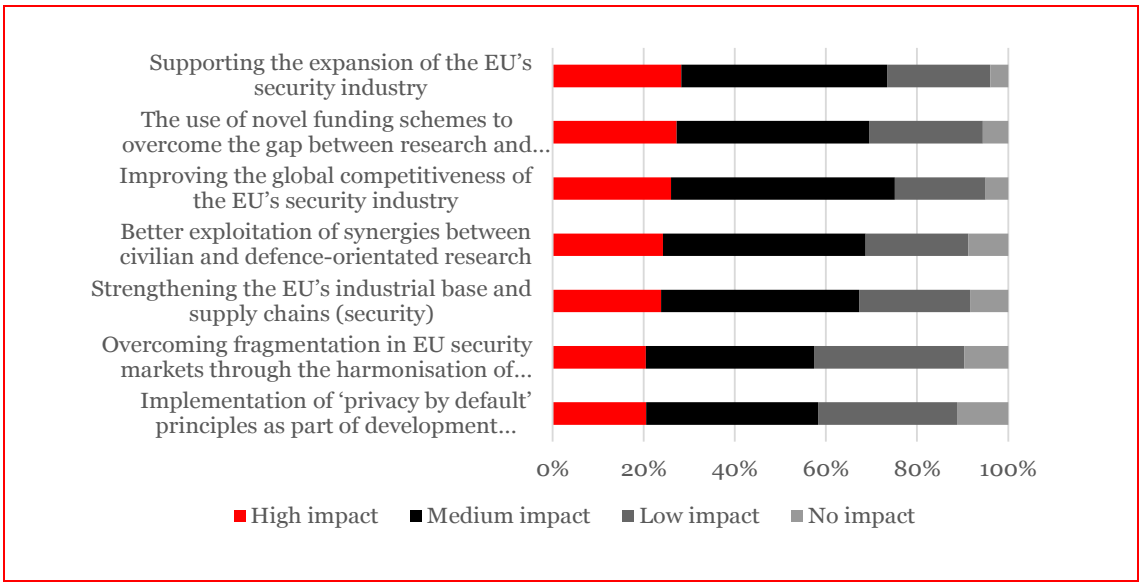
3.5.2 Impact in relation to European Security Industrial policy

EQ6. What are the impacts on the European Security Industrial Policy and on the security industry market?
Key indicator: % participants that judge the programme to have contributed to different dimensions of Security Industrial Policy; Share of stakeholders that judge the programme to have had an impact on the industrial policy

Participants were asked to assess the impact of the FP7 Security Research Programme in relation to European Security Industrial Policy and the security industry market.

Figure 15 presents the survey results and shows that a **majority of participants believes the programme has had a high or medium impact** on the EU's security industry and is improving the global competitiveness of the EU's security industry. There is slightly less widespread support for the programme's contributions to overcoming fragmentation in EU security markets and implementation of 'privacy by default' principles as part of development methodologies for security technologies.

Figure 15: What has been the impact of the programme overall in relation to European Security Industrial Policy and Industry Market? (n = 257)



Source: Technopolis participant survey, November 2014

The survey results **echo the sentiments of the majority of the interviewees**, wherein the great majority believes the programme has done a reasonably good job of engaging industry and has to a large extent provided a platform for dialogue between security businesses and the EU about the appropriate focus and shape of industrial policy. There were numerous additional remarks about the scope of the security industry, which is not captured by any single standard industrial classification and draws on the capacities and innovations in many other sectors of the economy from electronics to engineering: "some work to better map the extent of the value chains that may pay dividends for the programme in future, helping target calls for proposals and even NCP promotional activities." There was a sense in some quarters that Europe's large and powerful defence contractors had looked in part to the Security Research Programme as a means by which to compensate for tightening defence markets, and that this may be crowding out other more specialised technology firms coming in from other sectors with different kinds of solutions.

The interviewees were also positive about the programme's contributions to improving **connections between the providers and users of novel civil security solutions**; however, most noted that cooperation was still underdeveloped. Interviewees flagged the need for substantial further work to improve the connectedness of groups of end-users, to improve market efficiency through mutual learning, common standards, multi-client procurement or system-to-system connectivity. Stakeholders were more cautious about the programme's impact on industrial competitiveness, which they judge to have been positive, but still limited because of the manifold fragmented markets. Several individuals stated that they thought the European industry is continuing to lose ground to the very much larger companies in China, Japan and the United States, which benefit from larger, consolidated domestic markets.

The findings from the desk research, interviews and focus group (stakeholder) workshop all underlined the fact that Europe is not one market but many and that the **degree of fragmentation** makes it harder to do business and undermines international competitiveness as well. The fragmentation is partly institutional (political and legal differences between Member States and security actors), but there are also substantive interoperability challenges (organisational, semantic, technical). As such, FP7 has been helpful in bringing together communities – industry and end users – in projects that are helping to develop common concepts, terminology, open interfaces, middleware, etc. that will in turn facilitate improved multilateral and cross-border cooperation. In light of the potential importance of standardisation, this issue has been looked at more closely, and a quick review of the 307 security research projects reveals that almost 30% directly address standardisation issues in one way or another.

The case study on standardisation[46] describes these activities in some detail. The box below highlights a few points of interest from that case study.

Figure 16: Security research and standardisation

In the various areas covered by the FP7 Security Research Actions, standards can be used to reduce market fragmentation and improve interoperability between national systems.

- Security Research Actions have led to some interesting work in the area of standardisation, especially in **identifying gaps**, thus contributing to working towards reducing market fragmentation of the EU security market and to improved interoperability (for instance through the development of international common symbols for First Responders);
- Among the nine projects that involved a standardisation organisation, one (CRESCENDO) had a direct **impact on EU priorities regarding standardisation** in the field of security. It provided guidelines for the European Commission by identifying needs and gaps in standardisation. This was used as an input for a Mandate (M487**)**, given by the European Commission to the European Standards Organisations (ESO). It led the latter to focus their work on the following topics: CBRNE, border security, crisis management/civil protection.
- At the international level, ISO launched a new committee on security on 1 January 2015: ISO/Technical Committee 292 Security[47]. The launch of this committee is the result of the **increasing demand for standards on security at the international level**. Among the 27 members of the committee, all the biggest EU countries are represented. The focus of this committee has common features with the FP7 Security Research Programme (societal security, supply chain security, risk management, etc.). The objective is to develop a general model for broad security standards, with sector-specific issues dealt with in more specific technical committees. The establishment of **this new committee represents an opportunity for EU stakeholders** to use their project results to help set up international standards. This could be done by increasing the link between project partners and standardisation organisations.

Observations were made during the focus group (stakeholder) workshop that developing technical standards was not necessarily the most pressing issue for improving the efficiency of the many security markets in Europe, although the principles of standardisation are clearly critical to interoperability, and that a harmonised certification process was most urgent and would be a rather more expeditious means by which to allow manufacturers and service providers to demonstrate the fitness-for-purpose of their products. Reference was made to FP7 CRISP, launched in 2014, as an example of a highly relevant project that seeks to develop a robust methodology for security product certification that could be deployed in all markets.[48]

[46] For the executive summary and the complete case study see Appendix E and Appendix F respectively.

[47] ISO (2015), ISO/TC 292 Security and resilience.

[48] See http://cordis.europa.eu/project/rcn/185503_en.html and http://crispproject.eu/.

3.5.3 Impacts on the EU's scientific and technological research capacity

EQ7. What are the impacts on the EU's scientific and technological research capacity and leadership and on the European Research Area?
Key indicator: Number of publications, per million EC contribution; % of participants that judge the programme to have had an impact on different dimensions of scientific and technological research capacity; List of the main areas of impact on the scientific and technological research capacity cited by stakeholders

3.5.3.1 Partnership creation – impact on EU research capacity and leadership

The survey results and stakeholder interviews suggest that the programme has had a strongly positive impact on EU research capacity, simply because of its unprecedented investment capacity and its explicit focus on civil security issues. It was not possible to test this view objectively, as the evaluation team were unable to obtain a good estimate as to the overall scale of the **EU's security research capacity**, before or after the launch of the programme. So many of the participants are involved in multiple application areas and most may not even define themselves as security research organisations. The interview findings suggest that there are six EU Member States (Austria, Belgium, France, Germany, Sweden and the UK) with a national civil security research programme and perhaps another three (Italy, the Netherlands, Spain) that have issued security research calls within their technology programmes. Security is not a specific research priority for most EU Member States, and the EU Security Research Actions may account for more than two-thirds of total European public research investment in this field. Yet in areas like health or energy, the much larger EU programmes account for a far smaller proportion of total R&D expenditure overall.

On average, Security Research projects involved 12 different **participating organisations**. This is higher than the Cooperation Programme average of 11. The largest Security Research projects (on average) were in the 'intelligent surveillance and border security' mission area (16 participants per project on average), while the smallest were in the 'security systems integration' and the 'security and society' mission areas (10 participants per project).

Most Security Research projects involved participants from three (45%) or all four (42%) of the main **types of organisations** (HES, PRC, PUB and REC), while 11% involved just two types, and 2% only one. The average project (with 12 participants) also included participating organisations from seven different **countries**. Nearly all participations (91%) were accounted for by organisations in EU Member States, while among the other 20 countries involved, Israel, Norway and Switzerland stand out (together accounting for 7% of participations).

3.5.3.2 Volume and quality of academic outputs – impact on capacity and leadership

The evaluation team was not able to gain a good overview of the programme's contributions to Europe's leadership in security research.

Bibliometric and citation data from SESAM were not available; however, this type of information is not an especially useful means by which to test the international standing of applied security research. As already shown in Section 3.4.2, 41% of the 61 completed projects resulted in at least one publication, with 214 publications reported in total. This equates to 3.5 publications for every project assessed, or 15 publications reported for every €10m of EC contributions. These 214 publications were published in a very wide range of journals and other periodicals, including 110 different peer-reviewed **journals;** the majority of those 110 journals published just one or two FP7 Security Research-related articles.

The table below lists the 17 scientific journals that have accepted three or more publications from Security projects, sorted by the number of FP7 Security Research-related publications. Together these 'top' 17 journals (by number of Security Research publications) account for around 15% of the 110 peer-reviewed journals and over half (51%) of all the 214 publications reported.

Table 29: Top peer-reviewed journals, sorted by number of Security Research publications

Rank	Journal	SJR	No. pubs	% all pubs
1	Geophysical Research Abstracts		39	18.2 %
2	Defence and Peace Economics	0.4	9	4.2 %
3	European Journal of Political Economy	1.5	9	4.2 %
4	Journal of Geophysics and Engineering	0.5	6	2.8 %
5	Analytical and Bioanalytical Chemistry	1.2	5	2.3 %
6	International Journal for Ion Mobility Spectrometry	0.4	5	2.3 %
7	Analytical Chemistry	2.2	4	1.9 %
8	IEEE Transactions on Nuclear Science	0.6	4	1.9 %
9	Journal of Breath Research	0.6	4	1.9 %
10	Journal of Contingencies and Crisis Management	0.5	4	1.9 %
11	Carbon	1.8	3	1.4 %
12	Fire Safety Journal	1.0	3	1.4 %
13	IEEE Geoscience and Remote Sensing Letters	1.4	3	1.4 %
14	IEEE Transactions on Pattern Analysis and Machine Intelligence	7.6	3	1.4 %
15	Lecture Notes in Computer Science	0.3	3	1.4 %
16	Progress in Electromagnetics Research	1.4	3	1.4 %
17	Public Choice	1.1	3	1.4 %
	Total		**110**	**51 %**

Source: Technopolis analysis of CORDA data

Table 30 presents a different list of **'top security research' journals, this time based on the Scientific Journal Ranking (SJR)**[49] for each journal, rather than the number of security research papers published. The SJR provides an indication of the influence or prestige of the journal in question. The Commission uses an SJR of 2.0 or above in defining its 'higher-impact journals,' and in this analysis there are 23 papers (out of 214 publications in total) published in 17 journals with an SJR of 2.0 or above. For the great majority of security-oriented journals, the SJR index is below 2.0 and with almost 50% at 1.0 or less. That is not especially impressive, when judged against other (more research intensive) areas of the Cooperation Programme. That said, it can be imagined that the low scores reflect the publication behaviour of security research more generally, rather than security research in the EU, and one would see the same focus on rather narrow technical journals with low SJRs were one to run the same exercise for Germany or the United States, or any other country with a strong research and technology base.

Table 30: Top peer-reviewed journals, by journal rank indicator

Rank	Journal title	SJR	No. pubs	% of all pubs
1	Science	11.2	1	0.5 %
2	IEEE Transactions on Pattern Analysis and Machine Intelligence	7.6	3	1.4 %
3	International Journal of Computer Vision	7.0	1	0.5 %
4	Advanced Functional Materials	4.0	1	0.5 %
5	Small	3.4	1	0.5 %
6	Chemistry of Materials	2.9	1	0.5 %
7	Molecular and Cellular Proteomics	2.9	1	0.5 %
8	Environmental Science and Technology	2.7	1	0.5 %
9	Journal of Politics	2.7	1	0.5 %
10	Data and Knowledge Engineering	2.5	1	0.5 %
11	Journal of Conflict Resolution	2.5	1	0.5 %
12	Work and Stress	2.4	1	0.5 %
13	IEEE Transactions on Knowledge and Data Engineering	2.3	1	0.5 %
14	Optics Express	2.3	2	0.9 %
15	TrAC - Trends in Analytical Chemistry	2.3	1	0.5 %
16	Analytical Chemistry	2.2	4	1.9 %
17	Journal of Peace Research	2.0	1	0.5 %
	Total		**23**	**10.7 %**

Source: SJR SCImago Journal & Country Rank, January 2015.

[49] SJR is a journal-ranking indicator that measures a journal's impact, influence or prestige. It expresses the average number of weighted citations received in a selected year by the documents published in the journal in the three previous years.

Scopus assigns journals to 27 subject areas (major thematic categories), as well as 313 specific subject categories. The 110 different journals that publish Security Research Programme papers fall within just 19 **subject areas** (listed below). The top five (by number of publications) account for nearly two-thirds of the 214 publications resulting from the 61 fully-processed Security Research projects.

At first glance, it is surprising to see that 22% of publications have been published in journals linked with 'Earth and Planetary Sciences,' a distribution that is confirmed by the 39 items published in Geophysical Research Abstracts (GRA publishes short summaries of current research in the Earth, Planetary and Space Sciences in separate volumes). This distribution, however, underlines the importance of space-based infrastructure (remote sensing) to the development of new civil security applications, and the opportunity that affords academic partners to secure publications.

Table 31: Security Research Publications, by journal subject area

Rank	Journal Subject Area	No. Pubs	% of all pubs
1	Earth and Planetary Sciences	48	22.4%
2	Economics, Econometrics and Finance	27	12.6%
3	Chemistry	22	10.3%
4	Computer Science	20	9.4%
5	Engineering	19	8.9%
6	Social Sciences	14	6.5%
7	Biochemistry, Genetics and Molecular Biology	13	6.1%
8	Materials Science	12	5.6%
9	Medicine	9	4.2%
10	Chemical Engineering	6	2.8%
11	Physics and Astronomy	6	2.8%
12	Energy	4	1.9%
13	Agricultural and Biological Sciences	3	1.4%
14	Business, Management and Accounting	3	1.4%
15	Psychology	3	1.4%
16	Environmental Science	2	0.9%
17	Arts and Humanities	1	0.5%
18	Mathematics	1	0.5%
19	Multidisciplinary	1	0.5%
	Total	**214**	**100.0%**

Source: Technopolis analysis of CORDA data

Under the more detailed classification of '**journal subject category**', there are seven subjects that account for five or more publications each (and together just over one-third of all Security Research publications). These are:

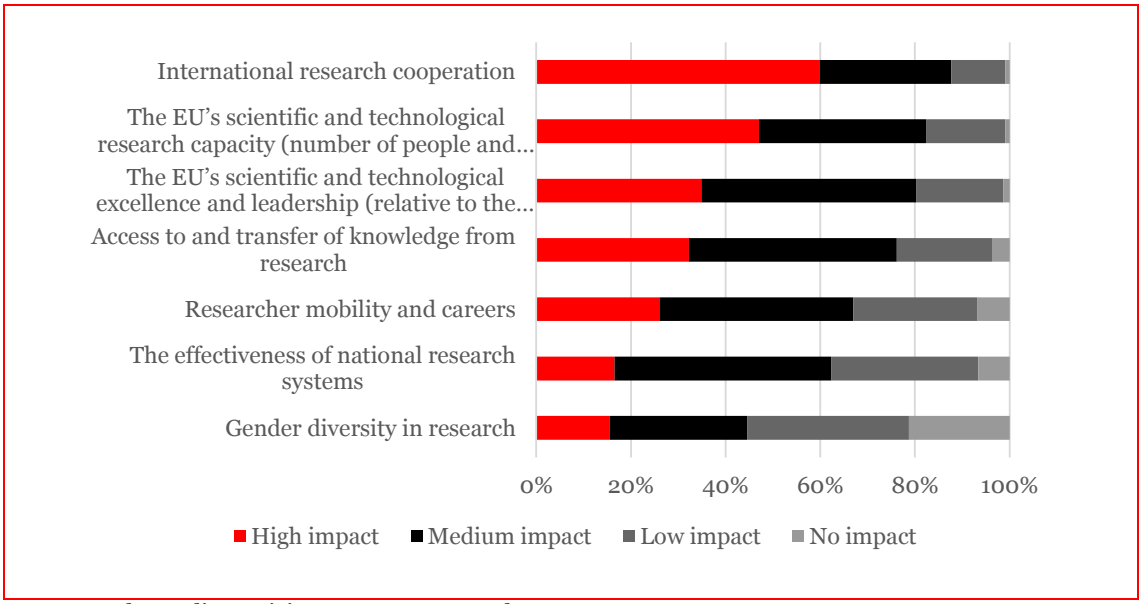
- Economics and econometrics (26 publications);
- Analytical chemistry (17 publications);
- Condensed matter physics (9 publications);
- Artificial intelligence (8 publications);
- Geology (6 publications);
- Spectroscopy (6 publications);
- Computer science – miscellaneous (5 publications).

Participants were asked to report back on and assess several other kinds of impacts, including the contributions of the FP7 Security Research Programme to the EU's scientific leadership or gender equality in research and several other ERA priorities. These topics overlap to some degree with the issues discussed in the sub-sections immediately prior to this, but are presented here again for completeness.

Figure 17 presents the results and confirms the view from multiple preceding analyses, whereby the great majority (88%) of participants judge the programme to have had a **substantial (high or medium) impact on international research cooperation**.

There is also widespread agreement regarding the programme's impact on the EU's scientific and technological research capacity (number of people and organisations) as well as the EU's scientific and technological excellence and leadership in the security research field. Participants are generally a little less positive about the programme's contributions to the realisation of the different ERA priorities, with a greater share indicating a low impact on, for example, researcher careers or the effectiveness of national research systems. This is understandable and reflects the fact that these issues are very much contextual for the FP7 Cooperation Programme overall. The results for gender balance are less defensible, as this was a priority for FP7; however Security Research is not alone in its poor performance on this dimension and the various gender-related supports and encouragements have all been strengthened for Horizon 2020.

Figure 17: What has been the impact of the programme overall on the following? (n = 259)



Source: Technopolis participant survey, November 2014

3.5.4 Value for money

EQ10. Do the actions under FP7 Security Research represent value for money?
Key indicators: Number of publications / IPRs / other outputs, per €10 million EU contribution compared to the average for the FP7 Cooperation Programme overall; FP7 Security results presented in a ranked list (scoreboard) alongside all of the other FP7 Cooperation Programme thematic areas

3.5.4.1 Output / impacts and expenditure – value for money

Value for money is a **difficult test to apply** to any EU research programme, since the classic ex post evaluations, such as the present study, are carried out at a point in time before most of the potential impacts have been realised, and this temporal issue is also complicated by the absence of any obvious alternative policy. In light of the fact that Europe is facing numerous serious security issues that are becoming more rather than less challenging, one cannot imagine the EU choosing to do nothing. It is also difficult to envisage any alternative policies that would be sufficient to bring about the reforms and improved performance of European public institutions and service providers, although the stakeholder interviews suggest that there is a need for a variety of other support measures ranging from support for standardisation to improved public procurement and pan-EU peer learning.

Given this intrinsic difficulty, it is typical for evaluators to look at a programme's productivity in terms of its ability to produce broadly similar numbers of technical outputs as **compared with other parts of the FP7 Cooperation Programme**.

On this test, output productivity, the Security Research Programme performs **rather poorly** in comparison with other parts of the Cooperation Programme, arguably reflecting the standard KPIs used by FP7, which emphasise research outputs (high impact journal articles) and IPR. None of these really capture the focus of the Security Research Actions, so it is no surprise that it sits in the lower quartile for all output KPIs. As was seen in Section 3.4.2, for every €10m of EC contributions (for the 61 completed projects recorded in the SESAM database), the Security Research Actions produced (amongst other types of outputs):

- 15 publications, including 2.3 publications in high-impact peer-reviewed journals;
- 1.3 intellectual property rights, including 0.6 patent applications;
- 1.5 other 'foregrounds' (e.g. other commercial exploitation of results);
- 163 dissemination activities.

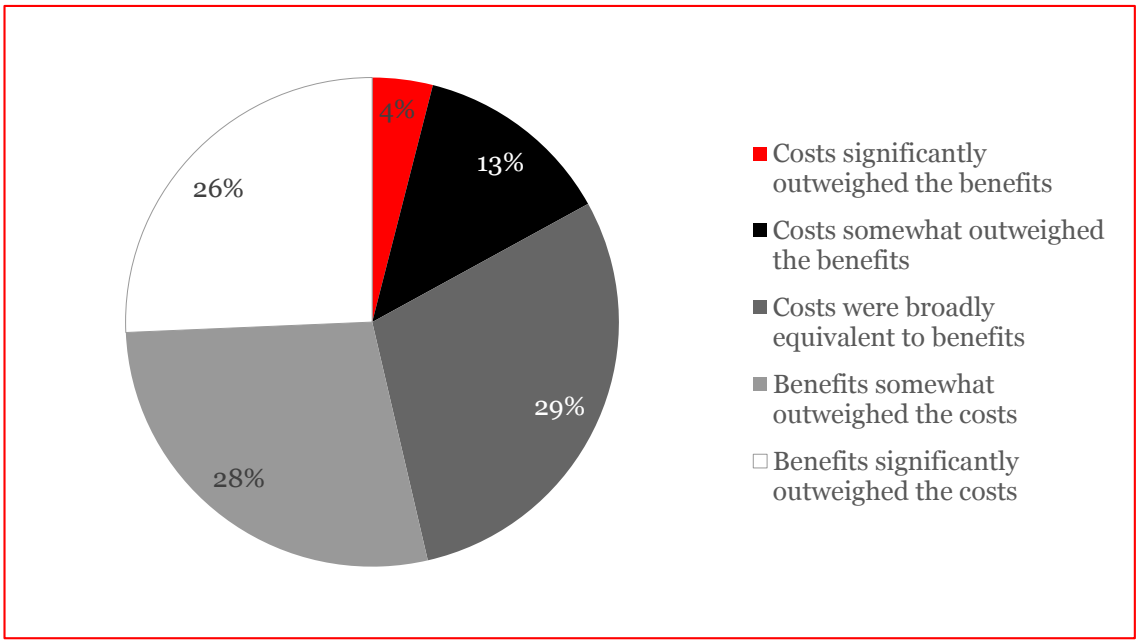
The comparably low level of exploitation and patents for FP7 Security Research may also be a result of the strategy to focus the SRAs more on integration than on the technologies needed for security applications that may exist already.

3.5.4.2 Comparison of cost and benefits

To address the difficult topic, also participants and stakeholders were asked to judge the programme in terms of its value for money, notwithstanding the possibility of a positive response bias.

Participants are also somewhat **ambivalent** about value for money, at least when looked at in terms of the balance between the costs and benefits of their own participation in the FP7 Security Research Programme. The figure below presents the results and shows that a small majority (54%) believe that the benefits outweighed the costs, while around 17% believe the costs outweighed the benefits. Around 30% believe costs are broadly equivalent to benefits.

Figure 18: Overall, how did the costs and benefits of participation in the FP7 Security Programme compare (n=506)?



Source: Technopolis participant survey, November 2014

The opinions gathered from the **stakeholder interviews were similarly mixed** on this question, albeit the great majority also commented that their view was partial and therefore rather impressionistic.

It was found that a small majority sees the programme as representing value for money because of the urgency of the issues it addresses and the need to create communities that are able to express their need for new technologies and to push for systemic innovation.

The academic interviewees expressed almost exclusively positive views, arguing that research is intrinsically valuable and that the benefits will emerge over many years in surprising ways and places.

End-users were split in their opinions, with one group praising the programme for getting these issues out into the open and creating networks and dialogue, while another group was rather frustrated by the disappointing results of their individual projects. Two end-users raised questions about value for money as judged by the cost of different activities, arguing that the staff days assigned to various activities seemed to be excessive.

Industry interviewees were similarly split in their views, with one half bemoaning the difficulty of making progress with saleable technology and the other group complimenting the programme on helping to move forward the state of the art in a more general sense.

3.5.4.3 Activities and expenditure – value for money

As noted previously (see Section 3.1.5, in particular Table 6), the Security Programme funded 307 **projects**, with an average EC contribution of €4.1m, and an average of €1.7m in leveraged funding per project (70:30 EC funding to leveraged funding, on average). The Cooperation Programme overall (including Security) achieved slightly higher financial leveraging, with its 3,779 projects attracting a (slightly lower) average EC contribution of €3.6m, and a (slightly higher) average of €2.0m in leveraged funding per project (which is a 64:36 ratio of EC funding to leveraged funding, on average). However, as explained further below (see Section 3.5.4.5), Joint Technology Initiative (JTI) projects distort the overall Cooperation Programme leverage rates.

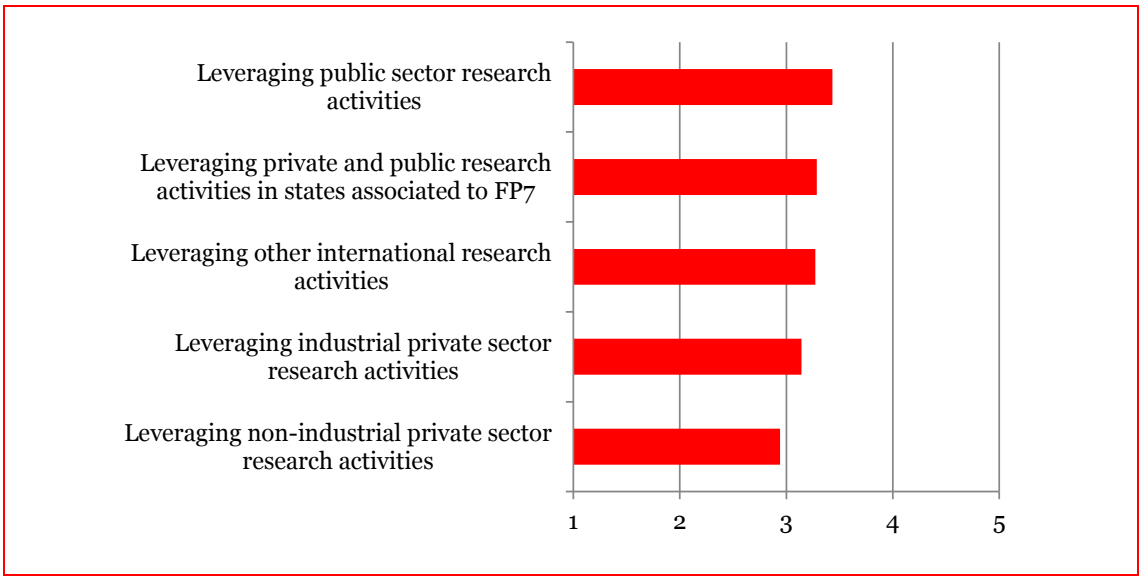
The financial leveraging is at similar levels when one moves from projects to participations. Security projects involved 3,741 **participations**, with an average EC contribution of nearly €338k per participation, and an average of €140k in leveraged funding per participation. Overall Cooperation Programme projects involved 86,854 participations, with a (slightly lower) average EC contribution of €323k per participation, and a (higher) average of €183k in leveraged funding per participation.

3.5.4.4 Leveraging of other research activities

EQ8. How effective is FP7 Security Research in engaging with and leveraging public and private research activities in Member and Associated States?
Key indicator: % of participants that judge the programme to be effective in leveraging other forms of research activity; share of stakeholders that judge the programme to be effective in leveraging other forms of research activity

Participants were asked to indicate the extent to which they judged their project had been effective in leveraging the research activities of other actors, by rating each of the dimensions on a scale of 1 to 5, where a score of 5 indicates that the aspect of research leverage was judged to be entirely effective. Figure 19 presents the results, with most areas of levering being judged to be around a '3,' 'neither effective nor ineffective.' Overall, the feedback suggests that projects have been somewhat **more effective at leveraging public sector research activities** and a little less effective at leveraging private sector research activities.

Figure 19: Indicate the extent to which your project was effective in leveraging the research activities of other actors (n = 377)



Source: Technopolis participant survey, November 2014. 1= not at all, 5 = very effective. Average rating shown.

3.5.4.5 Project funding – effectiveness of leveraging

The total estimated cost for all 307 Security projects combined was €1.78b, with the EC contributing €1.26b (or 71%) of the total. This compares to a rate of 64% for the EC contribution to the total costs of Cooperation Programme projects overall. This would suggest relatively low financial leveraging in the Security Programme. However, the figure for Cooperation Programme overall is heavily skewed by projects funded through the JTI Programme, where only 29% of total costs are met by the EC. Leaving aside JTI projects, the EC contribution across the Cooperation Programme increases to 70%, which is similar to the Security Research Programme rate. This implies that each euro contributed by the EC to Security Research projects attracted or **leveraged €0.42 of funding from other sources**. This is not particularly high or low compared with other parts of the Cooperation Programme, except the JTI Programme (see the table below).

Table 32: Total direct funding leveraged, per €1 of EC contribution

Programme	Total direct funding leverage
Joint Technology Initiative Clean Sky	€2.49
Energy	€0.72
Transport (including aeronautics)	€0.53
Nanosciences, Nanotechnologies, Materials and new Production Technologies	€0.44
Information and Communication Technologies	€0.42
Security	€0.42
General activities	€0.40
Space	€0.39
Health	€0.35
Food, agriculture and fisheries, and biotechnology	€0.35
Socio-economic Sciences and Humanities	€0.35
Environment (including Climate Change)	€0.34
Cooperation Programme (overall)	**€0.57**

Source: Technopolis analysis of CORDA data

Funding leverage varies by the **type of actor** within the Security Research Programme, as it does within all other areas of the Cooperation Programme, driven by differences in the rules regarding funding rates for different actors.

At the top-end, €1 of EC contribution leverages €0.54 from a PRC participation (on average) and €0.39 from a PUB participation. In absolute terms, the private sector contributed around €312m in matching funding, as compared with the Commission's contribution of €578m.

By comparison, €1 leverages €0.30 from a REC participation on average (€340m / €102m) and €0.29 from an HES participation on average (€257m / €75m), with those matching funds derived primarily from Member States' national research budgets. The overall leverage rate of €0.42 therefore depends heavily on the high proportion of PRC participations and financial support for the programme.

As presented in Section 3.4.2, of the 61 completed Security Research projects that have been assessed, 7% have been linked to national / international R&D programmes, while 2% were found to have an impact on promoting Joint Programming. None of the projects assessed so far have been found to have significant R&D participation from outside the EU, but nearly a third (31%) had involvement of non-RTD actors.

3.5.5 Appropriateness of the level of funding

EQ11. Was the level of funding of the FP7 Security Research Action appropriate for achieving the stated objectives?
Key indicator: Distribution of project value and EU contributions by general objective and by mission

3.5.5.1 Size of the programme

The feedback from the participant survey and stakeholder interviews suggests that the budget for the FP7 Security Research Actions was sufficient.

The majority of interviewees believe that the programme was of a **good size** and that the split by mission area allowed for a sufficient number of projects and some diversity in approach. A small minority (around 10%) argued that the programme was too small, and that this meant that quite large numbers of interesting projects of good quality had not been funded, and that the lower success rates weighed most heavily on participants from smaller countries. An even smaller number took the view that the budget was larger than had been required, and that halving the available funds would have had little effect on the programme's ultimate impact. These same individuals praised the programme's decision to build capability first before investing more heavily in major projects; however, they also expressed concern over the readiness of the community to deliver real improvements on the ground. Indeed, a significant minority noted their belief that the programme should continue to support smaller coordination and research projects and needed to be cautious about focusing on "mega projects." As in any series of interviews, the opposite argument was also heard, as a few contributors believed that these larger, multilateral projects have the scale and scope to cause real change to happen.

On balance, the evaluation team found evidence to believe that the programme was sized **appropriately** and that its strategy of focusing first on coordination actions and smaller research projects was judged positively. Given the continuing level of demand for funding and the escalation of security issues more generally, it also could be argued that there is a need for an increased budget in any forthcoming programme.

3.5.5.2 Distribution of funding by mission – level of funding

EC contributions to Security Research projects totalled more than €1.26b, but the distribution of these contributions across mission areas was not even. Three of the main security missions in particular accounted for an above average share of EC contributions: 'security of citizens'; 'security of infrastructures and utilities'; and 'restoring security and safety in case of crisis'. The three cross-cutting missions accounted for just 23% of EC contributions to the Security Research Programme, while the four main mission areas accounted for the other three quarters.

Across the Security Research Programme, the average EC contribution per project was €4.1m, and the average contribution per participation €338k. The table below shows equivalent figures for each of the individual mission areas, and highlights the above average contributions (shaded) to projects and participations in the four main security mission areas (1-4). In particular, in the 'intelligent surveillance and enhancing border security' mission, the contribution per project was 69% higher than the average, and the contribution per participation was 33% higher than the average.

Table 33: Average EC contributions per project and participation, by mission area

Mission areas	Average EC Contribution per project	Average EC Contribution per participation
Security of citizens	€4,210,406	€359,425
Security of infrastructures and utilities	€4,881,551	€350,647
Intelligent surveillance and border security	€6,957,413	€447,902
Restoring security and safety in case of crisis	€5,264,157	€394,991
Security systems integration, interconnectivity and interoperability	€3,209,994	€326,440
Security and society	€2,412,647	€236,732
Security Research coordination and structuring	€2,059,145	€175,907
(Other)	€197,495	€197,495
Total	€4,115,596	€337,741

Source: Technopolis analysis of CORDA data

3.5.5.3 Achievement of objectives – level of funding

As already noted, completed security research projects have been assessed by **project reviewers** (normally external experts) and project officers as to the extent to which they have achieved their objectives. Based on EC contributions to these projects:

- 37% of contributions are accounted for by projects 'fully achieving objectives';
- 56% of contributions are accounted for by projects 'mostly achieving objectives';
- Just 5% of EC contributions are accounted for by the three projects assessed as 'achieving some objectives, with corrective actions required'; and
- Just 2% of EC contributions are accounted for by the single project that has 'failed to achieve critical objectives'.

There is **no significant difference** in the average EC contribution provided to projects assessed within each of these different 'achievement' categories.

3.6 Evidence Building Block 5: European Added Value

EQ19. What is the added value of FP7 Security Research Actions?
Key indicator: Share of participants that judge the programme to offer high EU Added Value; List of key characteristics sorted in rank order, based on share of participants rating that aspect as being of high EU Added Value; Key aspects of EU Added Value identified by stakeholders; Key aspects of EU Added Value identified by end users

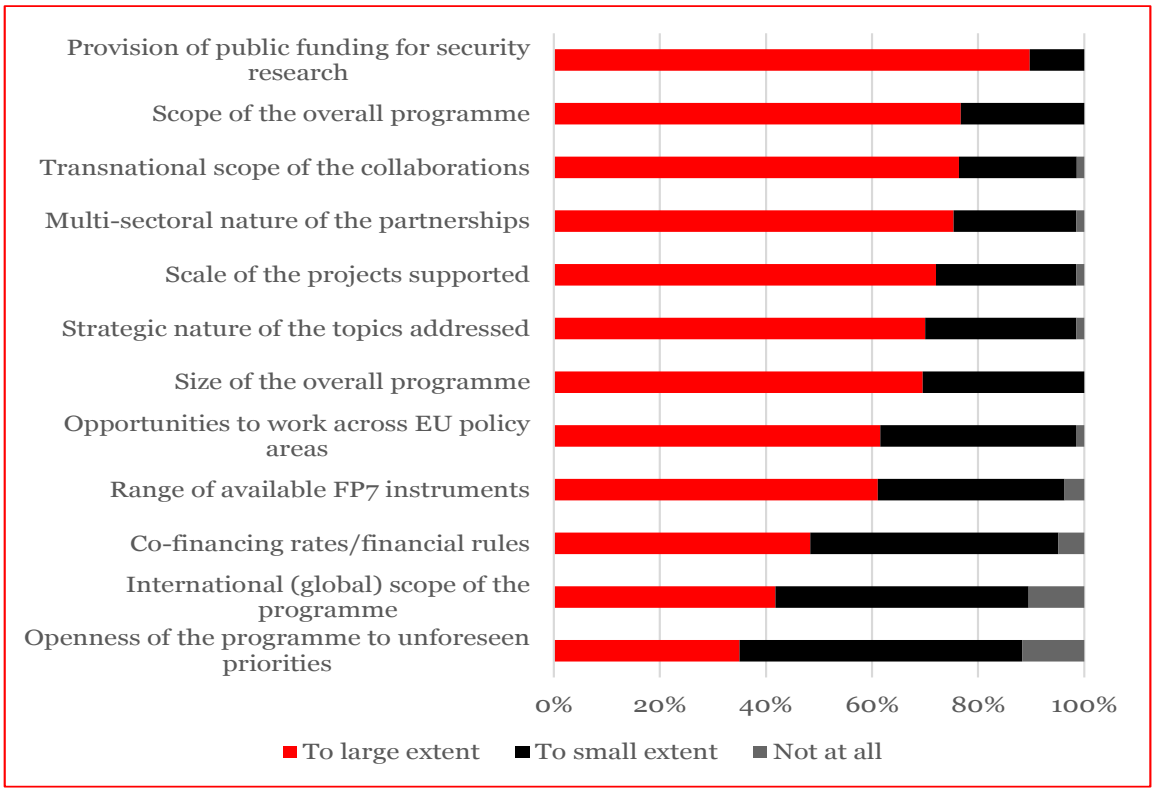
3.6.1 European added value of the FP7 Security Research Programme

For this evaluation study, **European Added Value (EAV)** was defined in pragmatic terms, as a benefit that cannot reasonably be achieved by the actions of individual Member States or private actors or which is likely to be substantially greater if pursued at an EU level rather than nationally or through some narrower territorial alliance. It points to the broader European relevance and significance of a programme for the EU, its institutions and policies. It is paramount in the formulation of the objectives and underlying ideas of research programmes initiated and supported by the EU.

In its simplest form, if one considers the EAV of a research programme to be about the scale and scope of the challenge, then the evaluation question needs to be posed at the European rather than the local level. It also needs to be considered in terms of policy inputs, given the importance of security issues in Europe and the fact that the low level of national security research investment creates a need for European action, in the short to medium term at least, until EU Member States possibly agree to fill the gap.

The results of the **participant survey suggest that there is a high level of EAV**, both regarding the European scope of the programme and the absence of national governments funding research on these issues, with around 50% of respondents stating that the programme has a high EAV in terms of the scope of its research questions. Coordinators were asked to indicate to what extent each of 12 qualities defined by the evaluation team apply to contributions to EAV of the FP7 Security Research Programme. The results are shown in Figure 20.

Figure 20: To what extent do the following aspects of the FP7 Security Programme provide (European) added value? (n = 85)



Source: Technopolis participant survey, November 2014

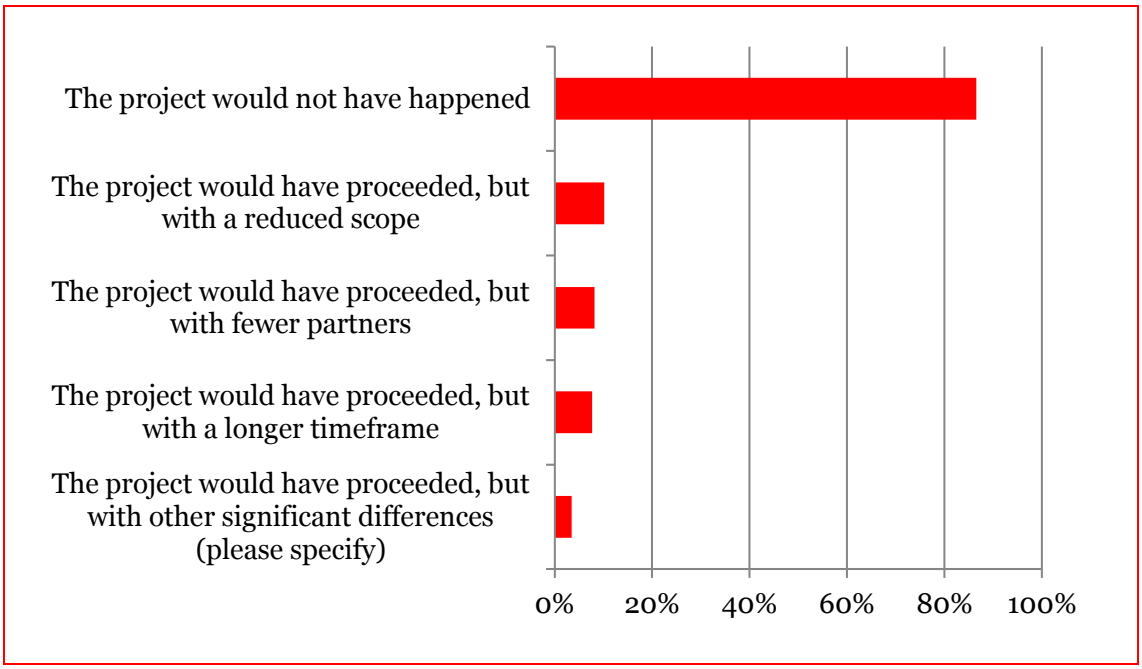
The responses show that the provision of public funding for security research is the most widely reported source of EAV, which corresponds with the feedback from the interviews. The results also show that the scope of the overall programme and the transnational character of projects are also both important sources of added value. To a lesser extent, the co-financing rates/financial rules, the international (global) scope of the programme and the openness of the programme to unforeseen priorities have added value. When comparing end-user responses to those of non-end-users, end-users are more positive in their assessments, with only one end-user responding "not at all."

3.6.1.1 Additionality

This study also addresses the extent to which the programme was supporting projects that otherwise would not have happened, with additionality more broadly defined. To that end, one of the questions in the survey invited participants to indicate what might have happened with their project in the absence of the support provided by the FP7 Security Programme.

Figure 21 presents the results of the responses to this question and suggests that the Security Research Programme is **highly 'additional'**. It shows that almost 90% of respondents believe their project would not have happened at all without the EU-funding.

Figure 21: What is likely to have happened in the absence of the support provided by the FP7 Security Programme? (n = 401)



Source: Technopolis participant survey, November 2014

This is a very high figure, even though it must be taken into consideration that this is a self-assessment. For the 10% or so of participants that believe their project could have proceeded, they imagine a project with a substantially reduced scope (e.g. fewer partners, less funding).

Qualitative feedback highlighted other differences, including the following examples:

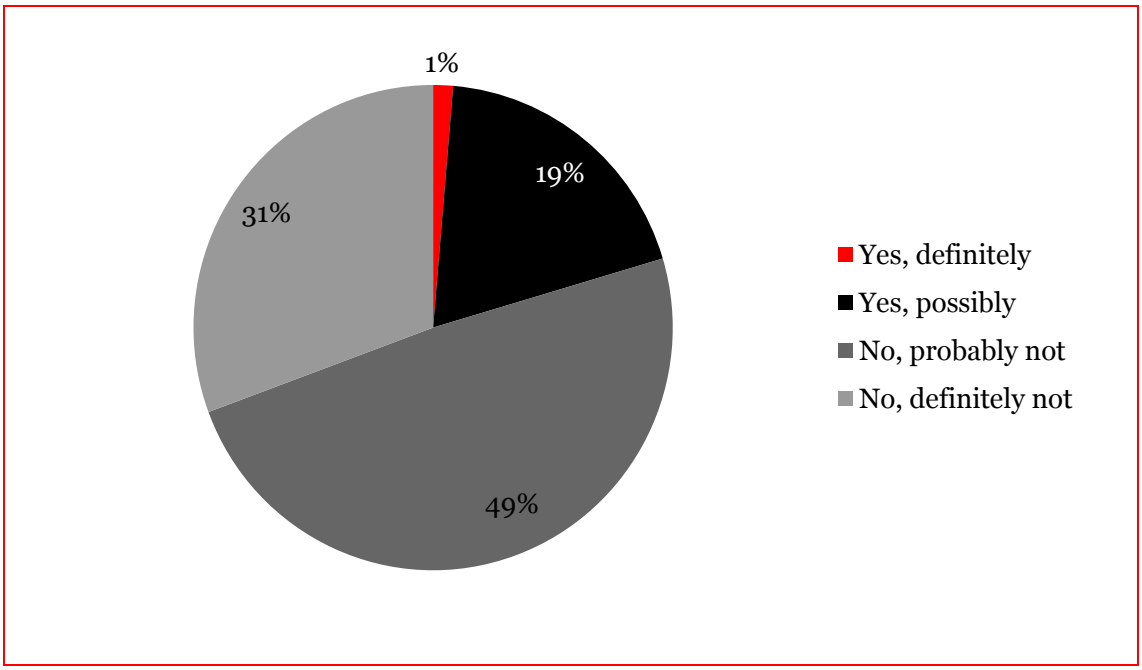
- "Maybe only as a national project, without the needed number of partners";
- "The international networking would be at a lower level";
- "Less research, less budget and therefore less interdisciplinarity".

When coordinators state that the project would have proceeded, but with other significant differences, the following examples are mentioned:

- "The project would have started with more focus on risk-based security";
- "The project would have been added to a commercial offering".

Respondents were also asked if their project could have been supported by an existing national or international funding scheme. Figure 22 presents the results and confirms the preceding analysis: it shows that a large majority (around 80%) of participants state that the **project would not have been supported by an existing** national or international funding scheme.

Figure 22: Could your project(s) have been supported by an existing national or international funding scheme? (n =362)



Source: Technopolis survey of FP7 Security Research participants, November 2014

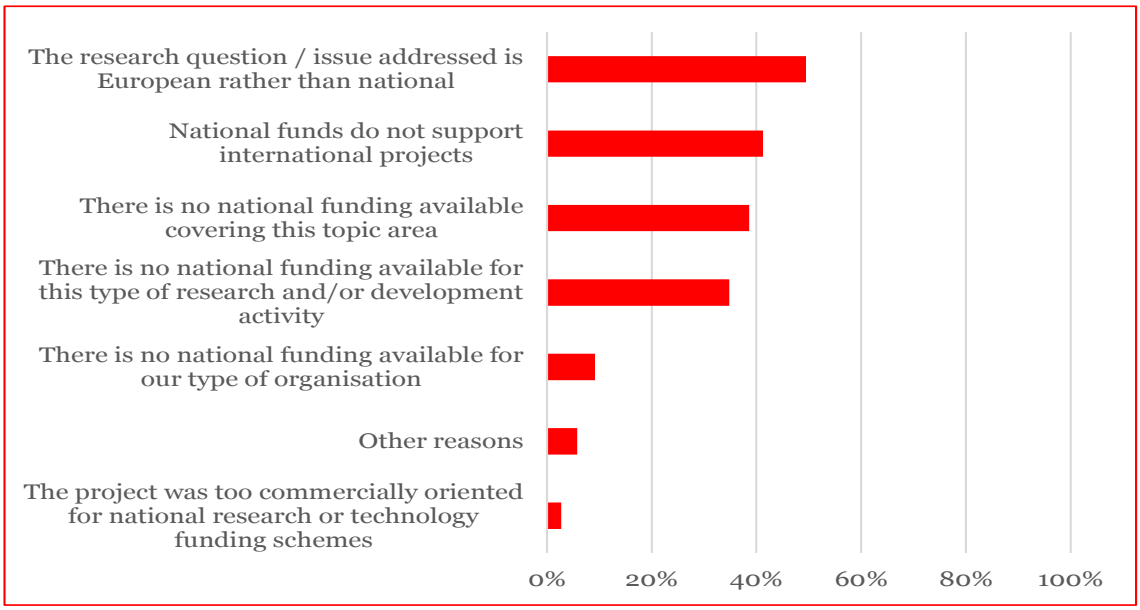
Where respondents answered "no" to the question above, they were asked to describe why not. This question produced very substantial amounts of feedback from the stakeholders, with a high degree of consistency among different types of **participants**.

The figure below presents the results, which strongly support the arguments made in the discussion of programme relevance, and suggest that there is **a high level of additionality and of European Added Value**. Nearly 50% stated that the research question addressed was European rather than national in scope, and therefore of limited interest and possibly ineligible for national support. Around 30% of the respondents stated that there is no national funding available for this type of research and/or development activity, national funds do not support international projects or there is no national funding available covering this topic area. A very small minority stated that the project was too commercially oriented for national research or technology funding schemes.

Other **reasons** that the participants chose to specify were, e.g.:

- "National schemes would not fund such an international network";
- "International aims of the project do not match scopes of national public funds";
- "There is a lack of funding for these types of multi-disciplinary projects";
- "European cooperation, i.e. different areas of expertise, was necessary";
- "This project required a large amount of funding support, which is just not generally available to social scientists".

Figure 23: If 'No' (your project could not have been supported by another scheme), why not ...? (n = 293)



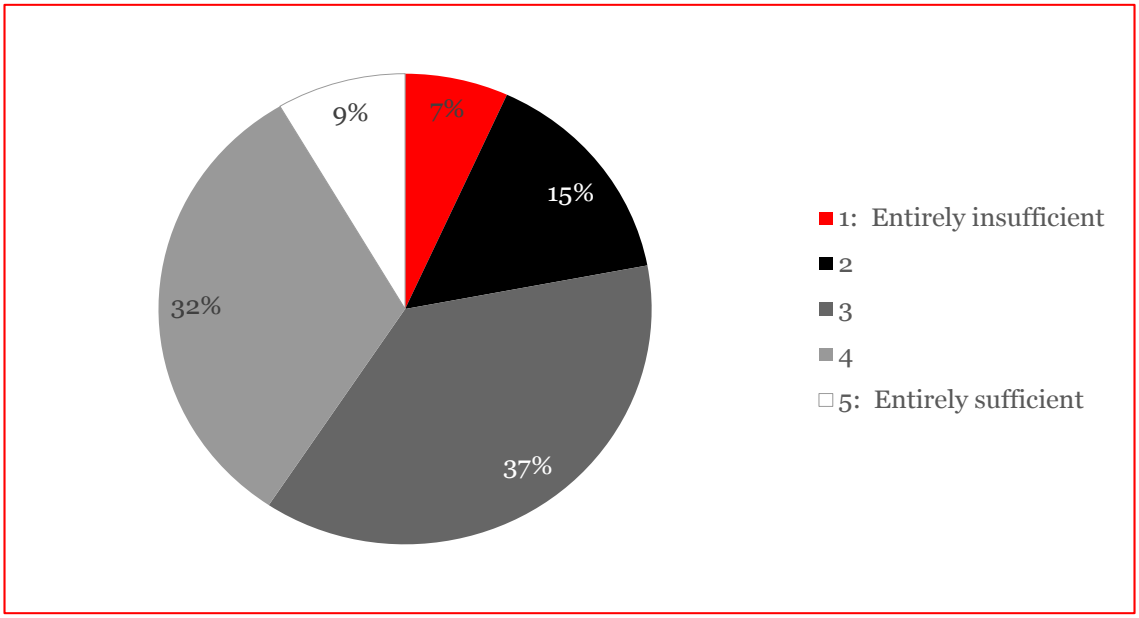
Source: Technopolis participant survey, November 2014

The views of the **interviewees** broadly reflect the opinions of participants, with the availability of research funds and the transnational nature of project teams being the two most widely cited sources of EAV.

3.6.1.2 Size of the budget

The coordinators were also asked if the FP7 Security Research budget was sufficient to achieve its stated objectives. The results are presented in Figure 24, which shows that the balance of opinion is essentially split: a small majority believes the budget was insufficient (53%), while a large minority (47%) believes it is sufficient.

Figure 24: To what extent do you believe that the €1.4b FP7 Security Research budget was sufficient to achieve its stated objectives? (n = 87)



Source: Technopolis participant survey, November 2014

The coordinators were asked to explain the reason for their answers and their comments have been aggregated in the following remarks:

- "There was more we would have liked to have done";
- "The budget provided the ceiling needed to select the best projects";
- "The right budget is difficult to evaluate without clear targets";
- "The budget was substantial, but the security challenges are even larger";
- "Some issues would have been better covered with an extensible budget".

3.6.2 Coherence

20. Are there overlaps/ complementarities between the activities evaluated and any other Community or Member State action in the relevant areas?
Key indicator: List of principal complementary Community and Member State actions; Key points of overlap or synergy identified by stakeholders

The interviews revealed a **broadly positive view** regarding the coherence of the Security Research Actions and their fit with other Community or Member State activities in the area.

This view is based on a general perception that there is a limited amount of activity under way within Member States with rather lower risk of overlaps or unnecessary duplication as compared with other parts of the Cooperation Programme. The interviews also served to recall the close involvement of Member States – through the programme committee – in finalising Security Research Work Programmes. DG HOME (previously DG ENTR) policy officers also consult with the other interested DGs on Work Programmes, which ensures a high degree of coherence between the various interests of the different Commission Services.

While interviewees expressed confidence that the programme is **broadly complementary**, they were not able to explain in any detail how the FP7 work fits with or feeds into the work of other programmes. The Security Research Programme covers a large number of mission areas, and the interviewees suggest that there is more or less Community and or MS activity in each area, and that it would be helpful to gain a better overview of the complete landscape.

Interviewees stated that there are numerous areas where work is going on in the MS or supported by other DGs, which come to light from time to time, but there is **no systematic overview** of such activities. This is mainly a legacy of the past when security was exclusively a matter of MS competence, while more recently it has become a shared competence, with the EU having the authority to initiative its own programmes. However, security research still remains something of a national legacy with a good deal of inertia, especially in the larger EU MS, which FP7 has been helping to overcome. The Commission's various inter-service activities help to ensure that there is more transparency regarding related EU-level activities.

No interviewee expressed the view that the Security Research Actions are in any way incompatible with other important initiatives in the area and might warrant refocusing.

Besides the FP7 Security Research Actions, there are a number of **national security research programmes**. In particular, the countries indicated in Table 34 below have dedicated civil security research programmes.

Table 34: National civil security research programmes (selection)

Country	Name of the programme
Austria	Österreichische Förderungsprogramm für Sicherheitsforschung *KIRAS* (National Research Development Programme)[50]
Finland	The National Security Research Strategy[51]
France	Concepts, Systèmes et Outils pour la Sécurité Globale *CSOSG* (Concepts, Systems and Tools for Global Security)[52]
Germany	Sicherheitsforschung – Forschung für die zivile Sicherheit (Security Research – Research for Civil Security)[53]
Italy	Progetto Interdipartmentale Sicurezza (Interdepartmental Security Project)[54]
Netherlands	R&D Programme on Security, Safety and Technology[55]
Sweden	Forskning för ett säkrare samhälle (Research for a safer society)[56]
United Kingdom	Research activities supported by different departments of government[57]

Source: Technopolis desk research

For a more in-depth analysis, a dedicated case study was carried out on the 'influence of FP7 SRAs on national research programmes'[58]. The main result of this case study is that national security research programmes are well aligned with the FP7 Security Research Actions. In particular:

- The programmes **focus** on the national needs of security research, formulated in line with their national priorities in the security area. While they have addressed a variety of security threats through the support of end-users, they also address the competitiveness of the security industry and, in two cases, the creation of new jobs. This orientation echoes important aspects of the FP7 SRA objectives;
- Anecdotal evidence points to the fact that national programmes have in some cases addressed short-term needs, compared to the longer-term perspective of the FP7 Security Research Actions. In other words, the programmes at national level have **complemented** the actions at EU level;
- Similarly, there is anecdotal evidence that national programmes have provided the opportunity for projects to **demonstrate the merit** of a technology, product or service first, before being taken up at the EU level and funded by the FP7 Security programme. The latter provides the opportunity to access larger markets;
- More generally, the analysis suggests that the national security research programmes have contributed to the **strengthening of networking and cooperation** in the Member States and in the European Union.

[50] http://www.bmvit.gv.at/en/innovation/security_research.html.

[51] http://www.intermin.fi/download/14209_national_security_research_strategy_.pdf?31652d691c05d188.

[52] http://www.agence-nationale-recherche.fr/suivi-bilan/ingenierie-procedes-securite/concepts-systemes-et-outils-pour-la-securite-globale/.

[53] http://www.bmbf.de/en/6293.php.

[54] http://security.cnr.it/index.php/en/.

[55] In the Netherlands, there has been the R&D Programme on Security, Safety and Technology and more recently an innovation programme 'Secure by Innovation', which includes funding for research on end-user needs.

[56] https://www.msb.se/en/About-MSB/Research/

[57] See for example the activities of the Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). Originally, a National Security Strategy and a Science and Technology Strategy for Countering International Terrorism, aimed to use innovation, science and technology to reduce the risk to the UK and its interests overseas from international terrorism.

[58] For the executive summary and the complete case study see Appendix E and Appendix F respectively.

3.7 Evidence Building Block 6: Conclusions on FP7 & outlook for H2020

21. To what extent could measures be taken to improve the positive effect of FP7 Security Research Actions and what measures would these be?
21. What lessons from the implementation of the FP7 Security Research Action could be drawn for the implementation of Horizon 2020?
Key indicator: Top 10 most commonly proposed 'valorisation' measures; Key 'valorisation' measures identified by stakeholders

3.7.1 Measures to improve positive effects of FP7 Security Research Actions

All respondents to the participant survey were invited to describe one practicable measure that could be taken in order to improve the positive effects realised from the FP7 Security Research Programme. Unfortunately, the very great majority of suggestions put forward would be relevant only to a new programme and did not constitute measures that could be implemented rapidly in order to extract greater value from the 307 projects supported under FP7.

The principal suggestions for **improving the impact of the existing portfolio** revolved around better programme-level support for dissemination and the creation of mechanisms to support the application of project results. This confirms the conclusion reached by a group of experts, in an internal pilot study on assessing project outcomes and their exploitation and usefulness of November 2013.

The stakeholder interviews produced broadly similar suggestions, with an emphasis on **clustering and additional events**. There is a sense that individual project seminars hold limited interest for the community at large, and that an event that brings together 10 or 20 projects from a broadly similar field, with much shorter presentations and more opportunity for direct interactions, could tip the balance, causing more policy makers, end-users and industrialists to invest their time and energy in a one- or two-day trip to Brussels or elsewhere.

The portfolio has a sufficient critical mass of projects to make this a possibility, and if it is done at a lower level than the programme (or even the whole mission area), it should still be affordable and achievable to run those events within the next 12 months or so. A programme conference such as the Security Research Events/Conference could be used for this purpose. In the meantime, it would be a positive development if the dissemination activities could be given a boost through additional funding for cluster events.

The focus group (stakeholder) workshop also emphasised the need for improvements to dissemination and valorisation, for both FP7 and Horizon 2020. The focus group had plenty of advice for Horizon 2020 as well, including simplification of administrative requirements, improved valorisation, improved cross-fertilisation among projects, improved support for high tech SMEs and the provision of follow-on funding to allow participants to progress to the next level on the road to full commercialisation. There was also a suggestion that rather more should be done to bring together end-users in order to better direct demonstration projects and even to help compare across competing solutions. The new public procurement instruments were welcomed, but were expected to struggle with the extent of the fragmentation on the demand side.

Project clusters may be a success factor for cross-project collaboration. A case study investigating the DEMOSEC cluster[59] highlighted several points of interest as regards clustering, including that it needs to be targeted on substantive issues of common interest and that it needs to be planned for and resourced in order to allow the self-evident potential value to be properly realised.

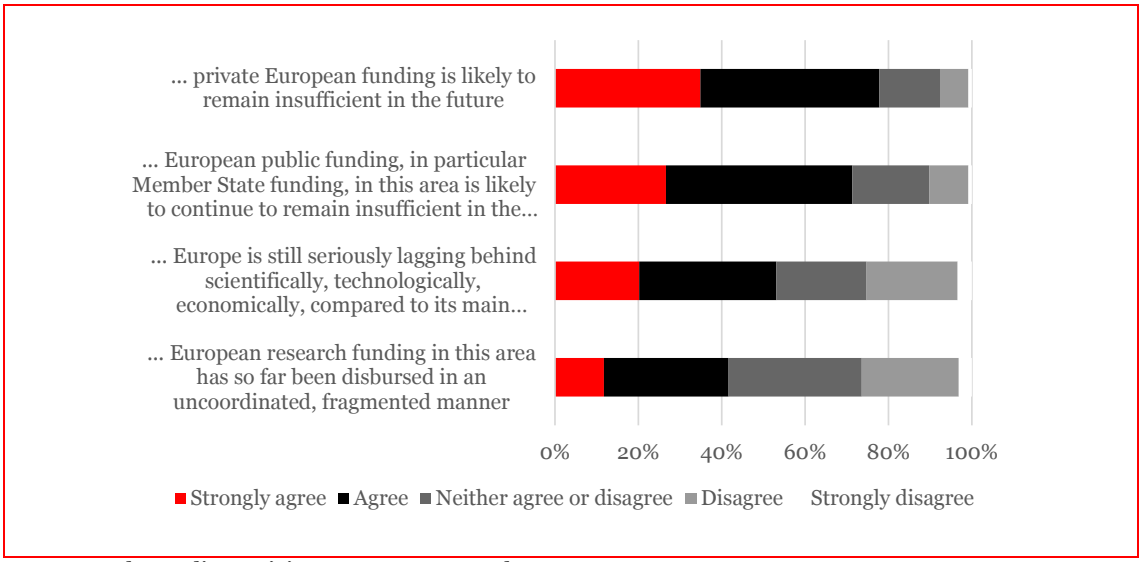
[59] For the executive summary and the complete case study see Appendix E and Appendix F respectively.

The Security Research Programme has also started exploring "clustering events" between projects within the Security Research portfolio itself. An example of this was a **virtual workshop** (January 2015) held with seven security-related projects to discuss and exchange views, knowledge and understanding of the Community of Users (CoU) initiative, which had been launched by the Commission in late 2014. Considered as a cross fertilisation workshop between the invited security research projects, the workshop focused on three key areas: Standardisation, CBRNE and Crisis Management. The Community of Users initiative is understood to be a mechanism by which better coordination of information exchanges of a general nature can be achieved and fragmented approaches are avoided.

3.7.2 Continuing need for EU funding of Security Research

All respondents to the participant survey were asked for their opinion on the continuing need for an EU security research programme, and were invited to indicate the extent to which they agree with a series of different statements. The following figure presents the results and shows that a large majority believes that private sector and **national research funding is insufficient** at the present time and is unlikely to improve sufficiently in the foreseeable future.

Figure 25: To what extent do you agree with each of the following statements as justification for the continuing need for EU funding of Security Research? Continued EU funding for Security Research is required because... (n = 570)



Source: Technopolis participant survey, November 2014

The stakeholder interviews added a further point in support of continued EU funding, namely the fact that most EU countries do not have national security research programmes. They therefore depend on EU money for sustaining and developing their research and industrial capabilities in the area of civil security.

3.7.3 Lessons learned

There were various lessons learned during the course of the programme, including how to make the 'responsible research' process work and how to accelerate the Security Scrutiny. The latter process has now been streamlined to such an extent that the Security programme's first call for proposals within Horizon 2020 has met the 240 day TTG target.

The programme has learned how to **engage end-users** through a broad range of promotional and project related activities, as well as through the wise decision to focus early calls on networking and coordination. The importance of enabling infrastructure and networks, to facilitate dialogue and articulation of research needs, has also become apparent. The great majority of stakeholders warn against complacency and argue that the Commission must continue to support these fledgling networks and strengthen interaction with end-users. The portfolio of projects and results provides the platform for going forward in this direction.

Clustering of projects is something that is also being experimented with, albeit only for a small number of projects in which there is a willingness to get involved with these wider endeavours. Notwithstanding this somewhat informal start, there appears to be substantial merit in looking to make more of this approach, both for the FP7 portfolio and for the new Horizon 2020 projects, increasing connections between projects such that there is greater cross-fertilisation of ideas and lessons learned.

Turning to survey respondents' advice for improvements to Horizon 2020, there was a high level of agreement among the several hundreds of responses submitted to the survey, and the following bullet points are a cross-section of examples of the rather brief suggestions participants think could be taken by **future programmes**:

- Reduce administration;
- Provide more funds / Increase budget;
- Funding for follow-up projects by rewarding best practices;
- Allow smaller consortia, ensure projects suit end-users'/industry's demands;
- Avoid overlaps in topics between projects/encourage collaboration between similar projects;
- Focus on presentation/implementation of results at the end of projects;
- Assist in/fund commercialisation;
- Obligatory meetings between similar projects to encourage exchange of experience;
- Fund new ideas/don't award multiple projects to one organisation;
- Be more flexible in terms of evolution of project;
- Allow continued funding.

Examples of measures that the participants think could be **taken by participants** are:

- Have a clear plan for exploitation/dissemination of results;
- Increase collaboration with partners/more focus on selecting partners;
- More user participation during project/uptake by end-users;
- Accelerated dissemination of project results (e.g. seminars, more publications);
- More flexibility with project timeframes;
- More active consortium/end-user participation/collaboration;
- Improved project management;
- Use project results for commercialisation;
- Continue to use networks/partners.

4. Conclusions and recommendations

4.1 Conclusions

4.1.1 Rationale

The general and specific objectives of the FP7 Security Research Actions correspond to the needs of EU stakeholders. This was **confirmed** through each of the study's data collection streams, from desk research and composition analysis to the participant survey and semi-structured interviews with stakeholders.

The great majority of participants, interviewees and workshop participants commended the **scope** of the FP7 Security Research Programme, strongly suggesting that the Commission did a good job in defining the mission areas. Another strongly positive factor was the evolving thematic focus to give greater weight to the issues of terrorism and cyber-security over the course of the FP7 programme period.

Overall, the programme attracted 1,790 eligible proposals and **funded 307 projects**, a ratio of around six proposals for every approved project (6:1), which is a good indication of the relevance of the Security Research Actions to the EU Security Research Community compared to the average for the Cooperation Programme (5:1). Demand outstripped supply as compared with all other Cooperation Programme thematic areas except social sciences (11:1) and ICT (7:1).

The participant survey confirms that every one of the programme's six specific **objectives** is relevant to one or more of the six categories of stakeholders. 'Developing the technologies and knowledge … to ensure the security of EU citizens' is the objective that is judged to be relevant for all stakeholders by the greatest proportion of all respondents (60%), whereas none of the objectives is seen as being of particular relevance to small and medium-sized enterprises (SMEs). Industry competitiveness is the objective with the least widespread endorsement of its relevance.

The seven **mission areas** are all considered to be relevant by 40-50% of the respondents to the participant survey. The stakeholder interviews and discussions at the workshop confirmed this view of the relevance of an EU security research programme and the appropriateness of its mission areas and coherence across different levels of programming, from overall objectives through individual Work Programmes.

4.1.2 Implementation

The programme was implemented **reasonably efficiently**, with participants applauding the introduction of various process improvements and simplification measures toward the end of the programme period.

There was widespread frustration regarding the **TTG** statistics, which are very much worse than the average for the Cooperation Specific Programme overall. It is understood that the major factor for this difference in performance is most probably the Security Scrutiny, a standard procedure unique to the Security Research Actions. The process has been looked at very closely and, as a result of some fine-tuning and intensification, the first call for Horizon 2020 met the new 240-day target for TTG.

FP7's introduction of additional **ethical review procedures** met with mixed reactions, with some feeling that the new tests have added costs without benefits and may even begin to exclude certain actors or types of work from future programmes, while others have welcomed the softening of the overly technocratic perspective of some security research.

The **move to the REA** went rather smoothly and there is a good working relationship between the dedicated teams in the policy unit in DG HOME and the executive agency. The policy unit has a small staff, and policy and project officers found outsourcing of part of the project management to the REA to be a very positive development, freeing up capacity to work more intensively on the development of the later FP7 Work Programmes, the preparation of Horizon 2020 and increasing space for interaction with other DGs and wider security interests.

The new arrangements however mean that the security policy team has a somewhat lower level of engagement with project-level activities, as only about a third of all projects are managed by the security policy unit. In the beginning, when many projects were transferred to REA, the security policy team had difficulties receiving information on them. However, the situation has improved, and the team also now has oversight of the two-thirds of projects managed by the REA (e.g. through access to project deliverables via FP7 IT tools). Yet there may still be room for improvement in the unit's awareness of some project-related activities. This is not a major issue for most R&D grant programmes, including FP7/ Horizon 2020; but it may be somewhat problematic in the area of security, where critical social challenges are being confronted by rather fragmented policy interests and institutional markets.

There was a good progression from early projects focused on developing awareness and networks to later calls, which have supported very much larger coordinated actions and platforms.

Regarding **dissemination** and **uptake of results** the study team concluded that individual project seminars hold limited interest for the community at large. The act of bringing together 10 or 20 projects from a similar security field to present their results could tip the balance, leading a much greater number of policy makers, end-users or industry actors to invest the time and energy in a one- or two-day trip to Brussels or another location to hear about research achievements and discuss opportunities. The Security Research portfolio now has a sufficient critical mass of projects to make this a possibility, and if it is organised at a lower level than the programme (or even the whole mission area), it should be affordable and achievable within the next 12 months.

4.1.3 Distribution of participations and funding

Three of the main security missions accounted for an above-average share of all projects, participations and EC contributions, namely 'security of citizens'; 'security of infrastructures and utilities'; and 'restoring security and safety in case of crisis.' The three cross-cutting missions accounted for just 23% of EC contributions to the Security Programme, while the four main mission areas accounted for the other three quarters. From the evaluation team's reading of the situation and feedback from participants and stakeholder interviews, this 'uneven' distribution does **not constitute an imbalance** in the portfolio and there are no fundamental gaps in the programme's coverage.

FP7 Security Research achieved more than double the **participation rate** by public bodies (non-research) as compared with the Cooperation Programme overall, reflecting also its focus on end users. Its level of industrial engagement also exceeded the average for the Cooperation Programme overall, while the involvement of higher education institutions was very much lower, both of which reflect the programme's support for capacity building and demonstration. The programme also comfortably surpassed the Commission's targets for SME engagement, notwithstanding arguments from some stakeholders that the support for SMEs had benefited private technology centres and consultancies more than the high-technology manufacturers. Both were present among participants, while the latter may benefit from further encouragement.

The programme supported a large number of actors from very many different countries, both from within Europe and beyond. Overall there were **48 different countries** involved in FP7 Security projects (on average 78 participations per country). The average project, with 12 participants, included participating organisations from seven different countries. Participation was skewed towards the larger EU Member States with established security research interests such as France, Germany and the UK. However, the ranked order of countries changes when one adjusts the number of participations and EC contribution for country size, with Luxembourg, Malta and Finland being the top participating countries. The top two non-EU Member States by number of participations and EC contribution are Israel and Norway.

The programme performed poorly on diversity, albeit its performance was in line with the Cooperation Programme overall. There are several sources of data on the **gender** of those involved in Security Programme participations – none of which is entirely comprehensive. Where known (96% of participations), the majority (83%) of lead scientific contact points for participations in FP7 Security projects were male, while just 17% were female. This rate was similar across all mission areas.

A majority of stakeholders believe the Programme has made good progress in its ambition to engage **end-users**. While the interaction is a long way from perfect, the intent is clear and the direction of travel positive.

4.1.4 Impacts of the programme on its specific objectives

The great majority of closed projects report that they have achieved all or most of their **objectives;** for the projects still running there is a high expectation that the objectives will be met. Advances in knowledge, new or improved technologies and improved security solutions are the results that are most widely reported. Around 20% of respondents have seen or expect to see their project result in policy outputs, market applications and standards, and new patents.

It is concluded that the Security Research Programme has had a **positive impact** on each of its specific objectives. The great majority of participants (75%+) hold this opinion. There is very little difference in the feedback, objective by objective. On balance, a greater share of participants believes the programme has made a substantial contribution to the 'developing technology to build capability' objective (85%).

Moreover, the team thinks that the programme has had a significant impact on the EU's **security industry** and is improving the global competitiveness of the EU's security industry. A majority of participants believe that the impact has been at least medium if not high. There is slightly less widespread support for the programme's contributions to overcoming fragmentation in EU security markets and implementation of 'privacy by default' principles as part of development methodologies for security technologies.

Importantly, it can be concluded that the programme has improved the **connections between the providers and users** of novel civil security solutions. In the survey participants expressed positive views about the programme's contributions in this regard; however, most also noted that cooperation was still under-developed. Interviewees flagged the need for substantial further work to improve the connectedness of groups of end-users to improve market efficiency, through mutual learning, common standards, multi-client procurement or system-to-system connectivity.

4.1.5 Impact on research capacity

FP7 Security Research is committed to supporting applied research of the highest quality, and in order to achieve that goal, it has sought to attract high-quality applications from strong project consortia including most of the EU's major security research groups.

The programme has **successfully attracted** many of Europe's leading national research laboratories and major security and defence companies. These are small in number and well known. Interviewees believe that the most active organisations have all been involved in the programme, a view they came to through attendance at events and the more general monitoring of the programme's project listings and calls. The findings of the desk research confirm this view. While there is no single list cataloguing Europe's leading security research organisations, a rapid reading of the top 50 participants reveals a 'Who's Who' of notable organisations with a longstanding interest in security-related research across the public and the private sectors.

The Security Research Programme has produced relatively **few research publications**, reflecting its focus on capability building and demonstration activities. One would expect this rather operational focus to be reflected in a preponderance of non-academic partners and a relatively low number of publications compared with other parts of the Cooperation Specific Programme.

FP7 Security Research has helped to expand capacity and shape the research landscape, with several pan-EU networks as well as national groups having been established. For **example in Ireland**, the FP7 Security Research Actions have allowed for the creation of the Irish Security Research Network, which includes about 950 academics, SMEs, large enterprises, civil servants, end-users, representatives of civil society, etc. The network has made a significant impact on the coordination of security research in Ireland, including improved transparency. The latter makes it easier for national authorities to attract investments and to foster cross-border collaboration between governments and companies.

The programme has also had a positive impact on Member State investment in security research, with several new national programmes having been created or expanded (e.g. Tekes Safety and Security programme, in Finland) and evolved (e.g. the collaboration and mutual opening up of the French and German national civil security research programmes).

4.1.6 Value for money

Value for money is a difficult test to apply to any EU research programme, and it is typical for evaluators to look at a programme's productivity in terms of the numbers of technical outputs per million Euros expended. It is also common for evaluators to ask participants and stakeholders to judge the programme in terms of value for money.

On the first test, **output productivity**, the Security Research Programme performs poorly in comparison with other parts of the Cooperation Programme, reflecting the standard KPIs used by FP7, which emphasise research outputs (high-impact journal articles and IPR). None of these indicators really capture the focus of the Security Research Actions, which as a new programme has had to invest heavily in building new pan-EU networks and knowledge exchange across end-users, industry and researchers. The conscious focus on issues of relevance to end-users has also given the programme a closer-to-market quality, and as such it is no surprise that Security sits in the lower quartile for all of the standard FP7 output KPIs. Finally, the comparably low level of exploitation and patents for FP7 Security Research may also be a result of the strategy to focus the SRAs on integration more than on the technologies needed for security applications that may exist already.

Participants are somewhat ambivalent about **value for money**, at least when regarded in terms of the balance between the costs and benefits of their own participation in the FP7 Security Research Programme. A small majority (54%) believes that the benefits outweighed the costs, while around 17% considers the costs outweighing the benefits. Some level of frustration is evident within each of the main groups of participants; however, end users were most likely to be critical, perhaps reflecting their inexperience with such transnational programmes.

The stakeholder interviews provided similarly mixed reviews, in which a small majority sees the programme as representing good value for money primarily because of the urgency of the issues it addresses and the limited capacity of Member States. The academic contributors almost exclusively held positive views, arguing that research is intrinsically valuable. End-users were split in their opinions, with one group praising the programme for getting security issues into the open and creating networks and dialogue, while another group was rather frustrated by the disappointing results of their individual projects. Industry similarly had split opinions, with one half bemoaning the difficulty of making progress with saleable technology and the other complimenting the programme on helping to move forward the state of the art in a more general sense.

4.1.7 Leverage

The programme performed **reasonably well** on financial leverage, securing an additional 30% of funding and contributions in kind, to match the EC contribution. This is in line with the performance for the Cooperation Programme overall, if one removes the Commission's Joint Technology Initiatives from comparison as these platforms were designed expressly to generate higher levels of private and national funding.

4.1.8 Level of funding

On balance, the evaluation team concludes that the programme was **sized appropriately** and that its strategy of focusing first on coordination actions and smaller projects was well judged. A small minority of interviewees argued that the programme ought to have been substantially larger, in order to allow maximum progress in all areas and in particular to give room for capacity building within the higher education sector. A rather larger number of interlocutors argued that the programme would have run an increased risk of 'wasting' funds, had it been larger, as a result of the finite capacity to execute projects. The development of these networks does however mean there is now a much larger community able to take forward this important research agenda. Given the continuing level of demand for funding, and the escalation of security issues more generally, the evaluation team would also argue for an increased budget in any forthcoming programme.

4.1.9 European Added Value (EAV)

The study team is of the view that the EAV of the programme is **rather strong**. The conclusion is supported by the results from all data gathering methods: the feedback from stakeholders, with a high degree of consistency across the many interlocutors and even among different types of actors, as well as the opinions expressed in the participants survey allow for such a conclusion.

4.1.10 Coherence

The FP7 Security Research Actions are judged to be a **good fit with other Community or Member State activities and policies** in the area, showing strong complementarity and with very few examples of unnecessary duplication. This is assured by the close involvement of Member States, through the Programme Committee, in finalising Security Research Work Programmes, and the work of DG HOME (previously DG ENTR) policy officers in consulting with other interested DGs, ensuring a high degree of coherence between services.

4.1.11 Maximising benefits from FP7 and outlook for H2020

There were various lessons learned during the course of the FP7 Security Research Programme, including how to make the 'responsible research' process work and how to accelerate the Security Scrutiny. The latter process has now been streamlined to such an extent that the Security programme's first call for proposals within Horizon 2020 has met the 240 day-TTG target.

The programme has learned how to **engage end-users** more effectively through a broad range of promotional and project-related activities, as well as through the enabling infrastructure and networks, to facilitate dialogue and articulation of research needs. The Commission should continue to support these fledgling networks in order to support the development of communities of practice and strengthen interaction with end-users.

Clustering of projects is something that is also being experimented with, albeit only for a small number of projects and in sub-fields where there is an evident willingness to get involved with these wider endeavours. Notwithstanding this somewhat informal start, there appears to be substantial merit in looking at doing more with this clustering approach, both for the FP7 portfolio and for the new Horizon 2020 projects, increasing linkages between projects so that there is greater cross-fertilisation of ideas and lessons learned.

The principal suggestions for **improving the impact of the existing portfolio** revolved around better programme-level support for dissemination and the creation of additional mechanisms to support organisations looking to apply results beyond the life of the project.

The focus group (stakeholder) workshop also emphasised the need for **improvements in dissemination and valorisation**, for both FP7 and Horizon 2020. The focus group had plenty of advice for Horizon 2020 as well, including simplification of administrative requirements, improved valorisation, improved cross-fertilisation among projects, improved support for high tech SMEs and the provision of follow-on funding to allow participants to progress to the next level on the road to full commercialisation.

There was also a suggestion that rather more should be done to bring together end users in order to better direct demonstration projects and even to help compare across competing solutions. The new public procurement instruments, such as procurement of innovation and pre-commercial procurement, were welcomed. Furthermore, there was strong support for help with certification to allow customers and contractors to meet on more equal terms.

Security research is strongly mission oriented and while there is demand for smaller projects – coordination actions, focused projects – there is also an appetite for launching bigger and more ambitious programmes, which have the scale to deliver impact on the ground. **Larger projects** permit a more strategic approach, involving all necessary stakeholders within the project's governance structures and providing the level of funding and latitude necessary to launch multiple complementary activities. Moreover, larger projects allow to encircle a problem, with networking, as well as market research or technology development projects or prototype services/demonstrations but possibly also normalisation projects or pre-competitive procurement. Oversight of these large initiatives is challenging and there is a risk that they will dissemble into a series of disconnected mini projects and key actors become disengaged. Hence, a strong leadership role by the Commission or by end-users would be required.

Moreover, the team concludes there is a need for **systemic overviews and linked research and innovation strategies**, which may help stakeholders understand exactly where a new technology offers a potential breakthrough in overall system effectiveness as opposed to just another new product that may offer some small incremental improvement in a narrow area of application.

In this context the issue of **project results** and their use by all project members, also following the end of the project by other participants in FP7 Security Research Actions, has to be critically reviewed. National laboratories and other technology centres absorbed a very substantial part of the total available budget in FP7, and yet end-users and industrial actors were very much concerned that the focus of development efforts and the intellectual property produced would remain inside these organisations and does not easily flow to end users.

4.2 Recommendations

This section lists recommendations developed by the study team. They concern the continuation and budget, the dissemination and uptake of project results, the shaping of the security research landscape, and the involvement of end-users.

4.2.1 Continue funding security research

The study team concludes that there is a strong case for **continuing to fund security research** under Horizon 2020, at a level that at least matches the scale of investment in FP7. It is recommended that the Commission develop a clearer overarching strategy for the programme which explains the nature of the challenges foreseen (e.g. in digital security) and what role an EU research programme can play in addressing these challenges. It would be helpful if these arguments could be accompanied by some more specific targets toward which the programme could be steered that ought to help ameliorate the effects of external buffeting by different stakeholders. The strategy and the broad investment plan could also cover the life of the programme.

It is recommended that the programme **focus** on the most demanding societal challenges, where a pan-EU programme can add most value. The cross-cutting issues addressed should be just that, horizontal considerations that are applicable to all activities, and not separate focal points in their own right.

The evaluation team recommends that the programme retain its commitment to **understanding** that innovation has as much to do with the systems, organisations and incentives, as it has to do with critical technologies. This points to a need to include additional research topics that address institutional settings and contexts for the use and application of technology.

4.2.2 Implement simplifications measures as planned in H2020

While numerous suggestions were received that invited the Commission to implement **further simplification measures**, many of those ideas have already been implemented in the transition from FP7 to H2020, which ought to reduce the administrative burden on participants. There are no further specific recommendations on this issue.

4.2.3 Continue promoting the Security Research Actions to SMEs

Promotion of the Security Research Actions to SMEs should be continued. The creation of the **new SME Instrument** is a helpful development, inasmuch as it enables individual businesses to apply for support at different points in the commercialisation journey (including help with access to finance) and without the requirement to collaborate with RTOs or indeed other businesses, unless that is beneficial. The shorter length of proposals, higher levels of funding and faster project lifecycles are also a better fit with the metabolic rate of the typical security research SME. The interplay between the mainstream research programme and the SME Instrument is not immediately evident from the research portal or the various guidance documents.

It is recommended that the Innovation and Industry for Security Unit consider developing a **briefing note** that National Contact Points and others might use when promoting security research to resident high-tech SMEs, and which would allow prospective applicants to be aware of calls for proposals in good time (e.g. the first call specifically for SMEs included a topic on critical infrastructure protection on urban soft targets).

SME intermediaries may be displacing other kinds of SMEs, possibly undermining the programme's ability to deliver improved EU security and EU jobs and growth. The dominance of technical consultancies within the SME cohorts of the EU RTD Framework Programme is well documented, but the risk of crowding out of other types of SMEs from important projects has not been properly assessed. The team recommends that the Commission launch a **small study** to look more closely at the positives and negatives of this evident skewedness within the FP7 SME participants and any implications for future Horizon 2020 calls for proposals.

4.2.4 Promote new models for the procurement of innovation

The creation of two **new models for innovation procurement** will be important for security research, offering a platform through which end-users can play a more influential role. Again, there is a lack of transparency regarding the links between these new instruments and current and future calls for security research proposals, as with the SME Instrument, and some further development of briefing materials for NCPs and other advocates would be helpful.

The new instruments for innovation procurement are of particular interest to end-users. They are key actors for the successful application of these instruments, as they enable field testing and intense feedback. Therefore, Commission should also provide end-users with specific information about the opportunities that the new instruments offer for them.

4.2.5 Consider the potential of a European Innovation Partnership for security

DG HOME shold consider the potential for developing a new **European Innovation Partnership (EIP)** focused on one of Europe's most pressing civil security challenges where cross border cooperation and the creation of stronger links between demand and supply sides will be most critical (e.g. cyber security).

The EIP model fits the needs of the security community rather well, inasmuch as EIPs support many different kinds of intervention, from research through to demonstration and on to public procurement as well as mobilising the demand side. They can also bring together prospective clients to help shape solutions without making individual commitments to buy and in helping producers and their supply chains agree on suitable technical standards that can help 'create' markets of sufficient size to be interesting. The lessons learned by similar efforts made in the past, as well as the current discussions of the Advisory Group of the Security Research Programme on this topic should duly be taken into account.

In this context it may be appropriate to reconsider the relative importance of industrial competitiveness within Horizon 2020's **overarching objectives** and to strengthen the significance of societal aspects in the objectives and the programme's rationale. In this context also legal, institutional and organisational aspects deserve further attention. In many cases, feedback from end-users suggests the required innovation is at least as much to do with the systems, organizations and incentives as with critical technologies. This points to a need to include additional research topics that address institutional settings and contexts for the use and application of technology.

4.2.6 Create more transparency about security research activities in Europe

While the team concluded that the EU programme was coherent with MS-level activities, there is a growing interest in security issues in more Member States and some additional work would be helpful to ensure coherence between EU and MS levels in the future. Hence, the study team concludes it is timely for the Innovation and Industry for Security Unit to develop a better sense of the wider landscape and the role of the EU security research programme within that context.

It is recommended that the Commission **map the security research landscape** (actors and activities), in which it is trying to add value (this has been begun on a limited scale by the Franco-German MAPPS initiative and even within FP7 projects, like the EDEN demonstration project and its work on mapping CBRNE research). It would cost little to catalogue other research and innovation policies and practices, and set up some kind of observatory to report on progress, achievements and issues arising. There are numerous precedents for this, whether relating to research on gender issues or regional innovation policy.

4.2.7 Explore additional ways to involved end-users

The Commission should continue to **strengthen the role of end-users** in security research. End-users have been increasingly involved in security research projects, mainly as participants and, in several cases, also as project coordinators. Moreover, they contribute important insights to evaluation and project review processes. The Commission should study ways to further buttress the role of end-users in all phases of the implementation of the Security Research Actions, including the project cycle i.e. the preparation of work programmes, the proposal evaluation, the project implementation and review phase, including an assessment as to the novelty of the envisioned output of research proposals. For example:

- At **proposal stage**, more end-users should be involved in the proposal evaluation process;
- The Commission could make it a mandatory requirement to involve end-users as direct project **participants** – rather than just in advisory bodies – in any project that aims to produce outputs above a certain TRL. Similarly, all projects should be required to set aside from the beginning a part of their budget for specific activities targeting end-users;
- The Commission should explore how end-users could play more active roles in the **dissemination** of project results and how they could be motivated to take up the results of other security research projects, e.g. by attending dissemination activities of other projects or by being actively involved in Communities of Users;
- End-users often have quite specific requirements that ask for an immediate solution, while the projects under the FP7 Security Research Programme have much longer timeframes. Therefore, the Commission should – across the different DGs – explore ways to provide quick **funding for innovation addressing the short-term needs** of end-users.

4.2.8 Improving valorisation of security research projects

There is a need to do more to maximise the **benefits** derived from the FP7 Security Research Programme and to reduce the tendency for insights and tools produced within projects to be left behind as partners move on to new projects or other priorities. It is recommended that the Commission consider hosting a series of FP7 Security Research **cluster events or symposia**, bringing together 10-20 project teams over one or two days, to provide the breadth of topics to give policy makers, end-users and businesses a good reason to attend such outcome focused events.

The evaluation concluded that value for money had been less than it could be, in part because this is a new issue for many and in part because the programme relied too heavily on individual projects to deliver value. The security research community is still a European community in the making, and as such there is a case for the programme itself to be actively promoting its activities and outputs, building knowledge sharing on the one hand, while also optimising impact on the other. The study team recommends that the Commission consider:

- **Clustering** H2020 projects to create focal points for the community to congregate around and gain value from the portfolio (dissemination and sharing of project results), make connections within communities and reflect on programme priorities;
- Identifying and focusing the clustering efforts on **specific topics** of shared interest. On those topics, organising work packages or targeted events would ensure genuine collaboration;
- Providing **funding** earmarked for collaboration, similar to network funding to cover transaction costs used in other areas;
- Encouraging project clusters to clearly **present** themselves as a joint entity, making clear their strong cohesion and inter-working;
- Increasing **support** for fledgling end-user networks, to strengthen their role in articulating research requirements, sharing good practices and generally raising the bar of performance across the board;
- Holding a **programme conference** for Security Research in Horizon 2020, possibly two, one at the mid-point and one in the closing stages of the programme.

Appendix A Evaluation questions (EQs)

Figure 26: The evaluation questions from the Technical Specifications

Relevance
1. Do the objectives of FP7 Security Research Actions correspond to the needs of EU stakeholders and were they adequately designed to contribute to the implementation of EU policies (i.e. the implementation of EU external policies, the creation of an EU-wide area of freedom, justice and security, and to policy areas such e.g. transport, health, civil protection, and environment?
2. To what extent did the objectives reflect (was there a clear intervention logic between) the levels FP, Specific Programme and Work Programme?
Effectiveness
3. To what extent did FP7 Security Research Actions meet their objectives? – What was the envisaged improvement in terms of security in the mission areas and what has been achieved? – To what extent did/does FP7 Security Research contribute to the overarching objectives of the Europe 2020 Strategy and the Innovation Union Flagship Initiative? – To what extent did/do FP7 Security Research projects contribute to improving EU competitiveness at international level and to European Security Industrial Policy? – To what extent were/are FP7 Security Research Actions successful in pursuing the general objectives of the Treaty, in terms of meeting the research needs of other Community policies?
4. What were/are the barriers, if any, to the effective implementation of the FP7 Security Action?
5. Are there any specific factors that render FP7 Security Research more or less effective than other actions?
6. What are the impacts on the European Security Industrial Policy and on the security industry market?
7. What are the impacts on the EU's scientific and technological research capacity and leadership and on the European Research Area?
8. How effective is FP7 Security Research in engaging with and leveraging public and private research activities in the Member and Associated States?
9. Were the results and their effects and impacts globally satisfactory from the point of view of direct or indirect beneficiaries and stakeholders?
10. Do the actions under FP7 Security Research represent value for money?
Efficiency
11.Was the level of funding of the FP7 Security Research appropriate for achieving the stated objectives?
12. Were the FP7 Security Research Actions implemented in an efficient way?
13. Are there major differences between the mission areas of FP7 Security Research? Are there differences as regards FP7 project types?
14. Did the actions attract the EU's best researchers or leading research organisations? Did the instruments reach the appropriate communities? What was the take-up for different types of actors – academia, enterprises, SMEs, etc?
15. Were there gaps or uneven distribution in terms of e.g. thematic areas, gender, and geographical coverage?
16. What aspects of FP7 Security Research are the most efficient or inefficient, especially in terms of resources mobilised by stakeholders?
17. What does this represent in terms of administrative and reporting burdens on stakeholders and other actors?
18. How could costs / administrative burden be reduced?
EU added value
19. What is the added value of FP7 Security Research Actions?
Coherence
20. Are there overlaps/ complementarities between the activities evaluated and any other Community or Member State action in the relevant areas?
Utility
21. To what extent could measures be taken to improve the positive effect of FP7 Security Research Actions and what measures would these be?
22. What lessons from the implementation of the FP7 could be drawn for the implementation of Horizon 2020?

Appendix B Tabulation of evaluation questions and EBBs

Table 35 groups the 22 evaluation questions, taken from the study Task Specifications, under the evidence building blocks (EBBs), picking out the key words from the full question, so the reader can grasp the main focus of the question without needing to process several hundred words.

Table 35: Tabulation of evaluation questions and EBBs

Evaluation Question No.	Topic of the evaluation question
Evidence Building Block 1 – Rationale	
1	Relevance
2	Intervention Logic
3	Meeting objectives
Evidence Building Block 2 – Implementation	
4	Barriers
5	Factors of effectiveness
12	Efficient implementation
13	Major differences between missions
16	Most efficient / inefficient aspects
17	Administrative burden
18	Possibilities to reduce admin burden
Evidence Building Block 3 – Achievements (Outputs)	
14	Attract the "best & brightest"
15	Gaps or uneven distribution
Evidence Building Block 4 – Outcomes / Impacts	
6	Impacts on Security Industrial Policy
7	Impact on ST research capacity
8	Leveraging other research activities
9	Global satisfaction
10	Value for money
11	Appropriateness of level of funding
Evidence Building Block 5 – European added value	
19	What is the added value
20	Overlaps / complementarities
Evidence Building Block 6 - Conclusions on FP7 and outlook for H2020	
21	Measures for improving effects of FP7
22	Lessons for H2020

Appendix C Typology of end-users

Building on the definition provided in the interim evaluation, it was proposed to define end-users in a strict sense as private and public organisations that may apply or make use of security technologies, equipment or services developed in an FP7 funded project in providing their security service of protection, support, aid, enforcement, emergency response, etc. While this excludes a number of organisations that are indirectly involved in security, such a definition provides a clear analytical basis.

In addition to "end-users in the strict sense", for the purpose of this evaluation, policy-making bodies were included in the end-user survey. Policy makers could be legislators or rule-making agencies using the results of security research for drafting regulations or agencies that develop strategies to address risks, e.g. lawmakers, nuclear safety agencies, atomic energy authorities or critical national infrastructure protection agencies, however not organisations defining overarching policies at a higher level.

Based on these considerations the following five categories of end-users were surveyed:

Table 36: Types of end-users addressed in the end-user survey

Type of end-user	Examples of sub-types	Main mission area where security services are provided
Emergency services	• Fire and rescue service • Emergency medical service • Lifeguard and lifeboat rescue services • Mountain, cave, mining, technical rescue • Bomb disposal • Blood/organ transplant supply	• Security of citizens • Restoring security & safety in the case of crisis
Public & private security services	• Police, regional, national, EU- and international (e.g. EUROPOL and INTERPOL) • National and European Customs and border control authorities for land, maritime security including coastguard, and aviation security, e.g. FRONTEX (border control) and EMSA (European Maritime Safety Agency) at EU level • Intelligence agencies • Public & private operators of surveillance systems	• Security of citizens • Security of infrastructures & utilities • Intelligent surveillance & border security
Operators of / companies with critical infrastructure	• Airport operators • Port authorities • Critical infrastructure such as power plants and IT-, Telco-networks • Road- and railroad networks • Metro networks • Facilities that might cause technological disasters, e.g. chemical plants, oil platforms	• Security of infrastructures & utilities • Intelligent surveillance & border security
Disaster relief and crisis management organisations	• Disaster relief management organisations • NGOs • International organisations	• Restoring security & safety in the case of crisis
Policy-making bodies	• Legislators • National authorities • Agency for nuclear safety • Agencies for critical national infrastructure protection	• All mission areas

Source: Technopolis

Appendix D Organisational affiliations of interviewed stakeholders

Table 37: Organisational affiliations of stakeholders who were interviewed[60]

Organisation	Stakeholder type	Country/EU
Scienvisic AB	Other stakeholder	Sweden
Polish Defence Holding	Industry	Poland
Greater Manchester Fire and Rescue Service	End-user	UK
GESA-German European Security Association	Other stakeholder	Germany
Guardia Civil	End-user	Spain
Laser Diagnostic Instruments OÜ	Other stakeholder	Estonia
University of Wolverhampton	Member of RTO	UK
INDRA	Other beneficiary	Spain
CDTI-Centro para el Desarrollo Tecnológico Industrial	Other beneficiary	Spain
DG ECHO	EU official	EU
TNO	Member of RTO	Netherlands
THW – Technisches Hilfswerk	End-user	Germany
APRE – Agency for the Promotion of European Research	Industry	Italy
EDA	Other stakeholder	EU
F.I.S. Security	Other beneficiary	Germany
EuroCrime Independent Research Centre	Other beneficiary	Italy
ENEA-Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile	Member of RTO	Italy
Bundesministerium für Forschung und Bildung (BMBF)	National official	Germany
Military Academy	Other stakeholder	Belgium
DG MOVE	EU official	EU
DG MOVE	EU official	EU
Satways	Industry	Greece
Danish Red Cross	Other stakeholder	Denmark
CTM-Centre of Maritime Technology	Member of RTO	Poland
EEAS	EU official	EU
European Parliament	EU official	EU
DG HOME	EU official	EU
Danish Ministry of Science, Innovation and Higher Education. Agency for Science, Technology and Innovation	National official	Denmark
National Defence College	Other beneficiary	Sweden
Thales Communications & Security	Industry	France
Vrije Universijteit	Member of RTO	Belgium
VDI Technologiezentrum GmbH, NKS Sicherheitsforschung	Other stakeholder	Germany
Frequentis	Other beneficiary	Austria
National Defence College	Other beneficiary	Sweden
FOI	Member of RTO	Sweden
SELEX	Other beneficiary	Italy
VINNOVA	National official	Sweden
Itrust	Other beneficiary	Luxembourg
ICTAF-Interdisciplinary Center for Technology Analysis and Forecasting	Other stakeholder	Israel
Austria Institute of Technology	Member of RTO	Austria
Tecnalia	Other beneficiary	Austria
LUXINNOVATION GIE	National official	Luxembourg
National Defence College	Other beneficiary	Sweden
Prosegur	Industry	Spain
Saab Group	Other beneficiary	Sweden
Austrian Academy of Science	Member of RTO	Austria
Fraunhofer INT	Member of RTO	Germany
Riga Technical University	Member of RTO	Latvia
Bundesministerium für Forschung und Bildung (BMBF)	National official	Germany
DG ENTR	Background	EU
Riga Technical University	Member of RTO	Latvia
DG ENTR	Background	EU
FFG - Austrian Research Promotion Agency	Member of RTO	Austria

[60] A number of interviewees (nine) were interviewed in their capacity as members of advisory boards of research projects.

Organisation	Stakeholder type	Country/EU
ÖRK-Austrian Red Cross	Other stakeholder	Austria
Bundesministerium für Forschung und Bildung (BMBF)	National official	Germany
Danish Armed Forces	National official	Denmark
DG HOME	EU official	EU
Netherlands Enterprise Agency	National official	Netherlands
Brimatech	Other stakeholder	Austria
Health Security Associates Consulting	Industry	France
Kemea - Centre for Security Studies	Member of RTO	Greece
DG ENTR	Background	EU
HITEC	Industry	Luxembourg
German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik)	Other stakeholder	Germany
Ardaco, s.r.o.	Other beneficiary	Slovakia
Vitrociset	Industry	Italy
DGA	National official	France
PRAXI Network/FORTH	Member of RTO	Greece
TEKNOLOGIAN TUTKIMUSKESKUS VTT	Member of RTO	Finland
RATP Group	End-user	France
Magen David Adom	End-user	Israel
Emergency Services College	End-user	Finland
EOS-European Organisation for Security	Industry	EU
Zaanstreek politie	End-user	Netherlands
University of Zilina	Member of RTO	Slovakia
DG TAXUD	EU official	EU
Centre for Defence Studies at King's College London	Other stakeholder	UK
Sateilyturvakeskus/Radiation and Nuclear Safety Authority	Other stakeholder	Finland
CEA-Commissariat Energie Atomique	Member of RTO	France
Police and Border Guard Board	End-user	Estonia
Euresearch	Other stakeholder	Switzerland
Dutch Forensics Institute	Other stakeholder	Netherlands
L-SEC	Other stakeholder	Belgium
Ben Gurion University	Other stakeholder	Israel
JRC-Joint Research Centre	Member of RTO	Italy
PIAP Poland	Member of RTO	Poland
PRAXI Network/FORTH	Other stakeholder	Greece
DG MARE	EU official	EU
ESRIF	Industry	Sweden
Greater Manchester Police	End-user	UK
APRE-Agency for the Promotion of European Research.	Other stakeholder	Italy
A.C.T. d.o.o.	Industry	Serbia
Hotzone Solutions	Industry	Netherlands
TNO	Other beneficiary	Netherlands
DG ENTR	Background	EU
DG TAXUD	EU official	EU
University of Helsinki	Member of RTO	Finland
Exodus S.A.	Other beneficiary	UK
Ametic	Industry	Spain
Belgian Federal Police	End-user	Belgium
Belspo	Other beneficiary	Belgium
Fed Police	Other beneficiary	Belgium
THW – Technisches Hilfswerk	End-user	Germany
DG ENTR	Background	EU
BBK	End-user	Germany

Source: Technopolis

Appendix E Case study executive summaries

This appendix presents the **executive summaries** of the **fifteen case studies**, developed as part of the final evaluation of Security Research under FP7. Details on the methodology are available in Section 4. The full text of the case studies is presented in Appendix F. The following table presents the list of case studies.

Table 38: List of case studies

No.	Title
1	Ethics in security research
2	Forms of end-user involvement in projects
3	Shaping the end-user landscape in the EU
4	Analysis of the complementarity of Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) research in FP7 and projects involving the European Defence Agency (EDA)
5	The FP7 Security Research Actions' impact on competitiveness of European security industry
6	Productive use of IPR from Security Research Actions
7	Demonstration projects
8	Protecting critical infrastructures – Port security
9	Tools, methods and resources to restore safety and security in case of crisis
10	The involvement of the citizen in security research
11	Project clusters – success factors for cross-project collaboration
12	Participation of smaller EU countries in FP7 Security Research Actions
13	Dealing with challenges in diverse project setting involving numerous types of partner
14	The significance of standardisation for Security Research Actions (pilot case)
15	The influence of FP7 Security Research Actions on national research programmes

E.1 Ethics in security research

This case study explores how ethics have been addressed through the FP7 Security Research Actions, at both a programme and project level, and what effect this has had. It examines the processes that have been put in place to identify and tackle potential ethical issues at the proposal stage, and looks at some of the specific mechanisms then employed by projects to address issues during implementation. It also considers in more detail a selection of projects dedicated to researching ethics and security. The case study contributes to the evaluation of the relevance and effectiveness as well as the efficiency with which ethics procedures have been implemented.

Consideration of ethics is important in any research, but this is particularly true for security research, where it is critical that products, process and systems developed for protection adhere to ethical standards and are socially acceptable. As a result, particular effort has been put into encouraging projects within the Security theme to take proper **consideration of ethics**. In fact, the Security Research programme has strengthened the attention given to societal issues like privacy and ethical issues across successive work programmes – both horizontally and through specific calls - reflecting a wider FP7 push, but also a specific shift in the Security Research theme.

Projects funded through all parts of FP7, including the Security Research theme, must adhere to fundamental ethical principles. To support this, the Commission has established a **standard ethics procedure**, which is used (to varying degrees) across the FP. Firstly, all applications pre-selected for funding that raise ethical issues must undergo an **ethics screening**, which results in an ethics screening report that indicates whether a more in-depth ethics review is necessary. The **ethics review** then evaluates all aspects of the design and methodology of the proposed project activities that raise ethical concerns, resulting in an ethics review report. Recommendations and requirements put forward in the ethics screening or ethics review reports are taken into account in subsequent grant negotiations and can lead to **obligatory provisions** in the conduct of the research. The types of issues most commonly identified for projects in the Security theme include research involving adult volunteers, research with potential for dual use, and issues relating to privacy.

The Security Research theme had among the highest number of ethics reviews of all Cooperation Specific Programme themes (behind only ICT and health). There were at least 90 undertaken in the Security Research programme over the FP7 period (2009-13). This equates to around a quarter of all projects funded in the theme, which is much higher than the 10% rate of ethical reviews seen in FP7 overall.

There are diverging views as to the **usefulness** of these standard procedures, and in particular the ethics checklist required as part of the proposal process. Some stakeholders consulted for the case argued it is just a bureaucratic requirement that serves little purpose, while others suggested it is not detailed enough, given the very complex nature of ethics in security. At the same time, some argued that the checklist is an important element in the proposal process, which helps researchers to pay greater attention to the potential ethical issues that may have a bearing on projects, and which can lead to useful further reflection and methodological adjustments.

There are then **mechanisms** employed by individual security research projects to ensure that ethical considerations are taken into account and tackled during project implementation. Two approaches examined in the case relate to establishing an **Ethics Advisory Board**, and to adding an **independent ethicist** to a project to oversee ethical concerns. Those applying these mechanisms have reported that they can add real value, particularly in ensuring that project outcomes are more socially accepted and justifiable. However, these mechanisms can also be quite costly – and so their inclusion is not thought to be justifiable or appropriate for all projects.

Under FP7 Security Research, ethics questions are also addressed directly through the funding of **projects in the field of ethics and justice**. Through this activity area the programme aims to address privacy, data protection and human rights issues, as well as acceptability, ethical issues and prioritisation. Increasing numbers of projects were funded in this area over the course of FP7 and, as of December 2014, there were eleven security projects focused on ethics, society and acceptability from a theoretical perspective. This still, though, represents less than 5% of all projects, participations and funding in the Security theme overall. This activity area is considered by stakeholders consulted for the case to be a highly relevant and important part of the Security theme, as other aspects of the programme are mostly technologically driven and industry focused. Specific ethics research work, it was argued, helps to counterbalance and complement the industry focus elsewhere by ensuring that research on ethics and security is advancing in parallel.

The case looks in more detail at three of projects funded within the ethics and justice activity area, and finds that they have successfully contributed to advancing knowledge in relation to social acceptance and justifications around security technologies. However, there was some concern amongst the stakeholders consulted that the results of the ethics-focused projects should be more widely disseminated in order to improve knowledge around ethics and security for the benefit of further research.

The case confirms that ethics needs to be an integral part of security research actions **going forward**, to ensure that project results are acceptable and socially justifiable. Continuing to include horizontal and vertical mechanisms that encourage the consideration of ethics is found to be an effective way to ensure this.

The FP7 Security Research programme has already made considerable progress in supporting greater consideration of ethics, and it is important that it continues to be strongly represented, both horizontally and at project level as part of future security research programmes. Several specific suggestions for the future were made, which relate to strengthening the focus and guidance on conceptual ethics; increasing funding to advance knowledge around ethics; encouraging follow-up by project officers of ethical considerations in projects; and more widely disseminating the results of specific 'ethics' projects.

E.2 Forms of end-user involvement in projects

This case study explores the extent to which end-users (i.e. authorities and organisations responsible for the security of citizens) have actually been involved in FP7 Security Research projects, and how they have been involved. It explores the benefits of this involvement. In particular, it looks at a selection of cases where end-users have assumed the role of project coordinator, and examines the approach taken in these cases to maximising the involvement and input of end-users. The case contributes to the evaluation of the relevance of the Security Research programme to end-users and the beneficial effects of their involvement.

The FP7 Security Research programme was conceived as a user-driven, application-based research programme. The importance of **involving end-users** directly in projects was therefore stressed in annual work programmes and applicant guidance.

While end-user participation in projects is not officially monitored, the overall evaluation suggests that this group of stakeholders has constituted a **significant minority** of the organisations participating directly in Security Research projects. They are also known to have engaged with the programme through other routes, such as project advisory groups and demonstration or dissemination events. Indeed, the study estimates that some 400 to 500 Security Research programme participants (a quarter of the total) are likely to have been end-users.

Most end-users who participated directly in projects **found the experience useful**, particularly as it offered increased opportunities for collaboration and networking, led to the development of new technological solutions, and provided improved knowledge, capabilities and understanding of security issues (amongst other benefits). However, despite the perceived usefulness of involvement and the range of benefits cited, less than 50% of end-users surveyed as part of the evaluation reported that the benefits of involvement outweighed the costs overall.

Common reasons for a **less than positive assessment** included: the excessive administrative requirements, poor cooperation within consortia, the lack of time and financial resources to produce desirable results, an insufficient (focus on the) uptake of end-results, and a lack of end-user involvement throughout projects. This last point was also particularly evident in the evaluation team's discussions with end-users.

A **main driver of end-user participation** in Security Research projects is an expectation that a solution to their specific needs can be found / developed, and that this can be deployed post-project in the operational environment. However, projects are felt to commonly fall short of this expectation. End-users have complained about the limited extent to which they are involved in projects – and particularly that they are often brought in only at the final stages (e.g. for prototype testing), when it is too late to input to the design and definition. This creates the potential for a gap between end-user expectations and the final output of the project, with results that cannot be deployed in the operational environment because they do not adequately correspond to real user needs. Ultimately, such gaps can have a negative impact on the relevance, and therefore effectiveness of projects, and the likely uptake and impact of results.

Linked closely to this is a perception that **project ideas are often driven by partners from research organisations and academia**, who define project objectives, the intermediate steps needed to achieve the results and the structure of the project. Only then does a search take place for end-users to involve in the consortium and provide support for the testing phase. As a consequence, testing is the only moment in which end-users can provide feedback to the technology developers and input specific requirements for the product, and this can be too late.

The study has identified a small number of end-user organisations that have taken a more pro-active approach to influencing project outputs and strengthening the involvement of end-users, by **assuming the role of project coordinator**. Three of these projects have been looked at in more depth, and show a different and deliberate approach to maximising end-user involvement and input in projects, helping to reduce or remove the gap between end-user expectations and project results. **Features of end-user led projects**, include:

- End-users are involved from the beginning of the project to define the operational requirements of the tool / product to be developed;
- End-users are placed in charge of specific work packages, often aimed at identifying requirements and proposing potential solutions and guidelines;
- End-user involvement is sought throughout the duration of the project, and not only during the testing and validation activities;
- End-users outside the consortium are also actively involved and consulted, e.g. by including them in the advisory board or through interviews;
- The project explicitly seeks to develop and deliver a product that is fit for purpose from the point of view of end-users and not that of research performing partners;
- Communication and dissemination are deliberately targeted at end-users.

Building on the experiences and efforts of the FP7 Security Research programme, and to ensure that the strategic objectives of the programme are achieved, **the future** H2020 work programmes and calls for proposals should include provisions to encourage end-user participation throughout the programme and maximise end-user input. Furthermore, considering the specific nature of the security domain, often dominated by sudden threats requiring very fast response capacity, the inclusion in H2020 of faster funding procedures in case of immediate threats might also contribute to the overall capability of end-users to respond to threats to citizens' security.

E.3 Shaping the end-user landscape in the EU

This case explores how the FP7 Security Research Actions stimulated the cooperation of providers and users of civil security solutions by examining the experience of organising communities of end-users in three sectors: customs; disaster risk and crisis management; and law enforcement. It contributes to the evaluation of the involvement of end-users and barriers to effective implementation of Security Research Actions.

The Security Research programme was conceived as a **user-driven, application-based research** programme, which would stimulate the cooperation of providers and users for civil security solutions, and deliver mission-oriented research results to reduce security gaps. End-user involvement was seen as a way to achieve a better-targeted programme and projects, and to develop and deliver innovative solutions that could be deployed in response to security threats. The engagement of end-users was also important if these intended beneficiaries were to gain access to, and extract benefit from, relevant and appropriate technologies and solutions produced.

Consequently, one of the major benefits of the FP7 Security Research Actions has been the impact that the programme has already had on the end-user scene. Not only have large numbers of end-users become involved as project participants, coordinators or advisors, but within certain sectors, they have also started to organise themselves into **coherent and active communities**. This case has examined three such groups:

- The **European Customs Detection Technology Expert Group** (CDTEG) was created in 2011. It serves as a platform for (i) sharing information between customs technology experts, and (ii) the end-users of security technologies to define the needs for new and improved technologies. Outputs from the first period of the group's operations have provided a basis for discussions between EU customs administrations and the EU security industry, research institutes and academia, as to future R&D activities and their alignment with end-user requirements and needs. Inputs from the CDTEG process were also formally communicated to the FP7 Security Research programme, such that they might be taken into consideration in work programmes and calls. This has already translated into better-defined work programmes and topics, as well as specific projects addressing the needs identified by the Group. The Security Programme Committee lacks specific and technical knowledge of threats and needs in the customs sector, and so the input from the CDTEG provides an important source of insight into the real needs of end-users, which might otherwise not exist.
- The **Community of Users (CoU) on Disaster Risk and Crisis Management** held its first meeting only in 2014. It responds to the diffuse nature of disaster risk and crisis management policy and to the diversity of actors in this field by (i) providing a common platform for sharing information, and (ii) bringing together key scientific, policy and industry actors, as well as end-users, around a common vision and strategy. It is intended as a means to share information between different stakeholders on research and policy developments, to promote greater alignment and complementarity in approaches to research and policy, and ultimately to stimulate common demands. The twice-yearly meetings of the group will ensure that new research information and policy updates are made widely available, and that different actors are aware of developments in different fields. It is hoped that the Community of Users will become an essential supporting group, whereby various actors will cooperate to boost the implementation of research outputs, and improve EU policy implementation.

- The **European Network of Law Enforcement Technology Services** (ENLETS) was set up in 2008. It is a platform to share information and maintain communication channels between national law enforcement agencies (end-users responsible for implementing new technologies in police departments within Member States) and those parts of industry, research and academia with an interest in the development of law enforcement technologies. It serves as a central contact point for Member States, research and industry, agencies and the European Commission, as well as providing a technology watch function for internal security research and industrial policy tasks in Europe. The network has already supported a changed approach towards innovation and technology within Europe's police forces, which can be seen for example in the inclusion of innovation and technology assessment within police policies. It is anticipated that ENLETS will go on to play a more fundamental role in coordinating and supporting the actions of law enforcement forces at EU level with regard to research and innovation, in strengthening the involvement of end-users in both EU security research activities and industrial policy, and in closing the gap between technology providers, the research community and end-users.

These examples show that organised communities can provide end-users, research organisations, industry and policy makers, with **a forum to share information, technical specifications, needs and ideas**, so as to achieve better programming, more effective project results and faster uptake of developed technology. They offer a better understanding of the operational needs of end-users, better coordination of research actions, an increased likelihood that project results will be taken-up, and increased involvement of end-users in developing solutions to their specific needs. Such end-user communities are therefore becoming key players in the EU security policy framework, with policy making and programme implementation processes benefiting from the ability of end-users to effectively coordinate and communicate not only with EU Institutions, but also with the research community and industry.

Nevertheless, the wider evaluation has found that the high level of complexity of security policy, together with the wide variety of research projects, difficulties in bridging the gap between innovative products and the market, and the absence of communication channels between policy makers, end-users and technology providers, continues to create problems for the effectiveness of the actions funded by the FP7 Security Research programme. As such, there **continues to be a need for better coordination and involvement of end-users** in the design, delivery and exploitation of Security research – both at the project and programme level.

As for **the future**, the already important role that certain Communities of users play in the EU policy making and programming process should be strengthened and formalised under Horizon 2020, and expanded to other end-user sectors. A stronger role for end-users communities in the EU policy making and programming process would allow targeting specific threats in the most effective way, as well as allow better access to the market for the technologies and products developed by the projects.

E.4 Analysis of the complementarity of CBRNE security research in FP7 and projects involving EDA

This case examines the complementarity of research projects funded by the FP7 Security Research Actions, on the one hand, and projects overseen by the European Defence Agency (EDA), on the other, about chemical, biological, radiological, nuclear and explosive (CBRNE) hazards. In as much as the EDA oversees projects funded and pursued by its members, the case explores how effective FP7 Security Research is in engaging with and leveraging public and private research activities on CBRNE in the Member States. Given that the FP7 Security Research programme has a strictly civilian character and the EDA focuses on cooperation in the military area, this case also addresses the question of dual-use[61]. The case contributes to the evaluation of the coherence of the programme with the research activities of Member States.

[61] Dual-use items are defined as goods, software and technology normally used for civilian purposes but which may have military applications. A considerable number of technologies and products are generic and can address the needs of both civil and military end-users, especially at lower technology readiness levels. CBRNE hazards represent one area

Research and demonstration efforts within FP7 in CBRNE and natural and man-made disaster management areas are directly or indirectly **supporting the implementation of key EU policies**. In addition to this, within the framework of the European Defence Agency (EDA), research projects are also conducted for CBRN protection, which are coordinated with DG HOME under the so-called European Framework Cooperation (EFC).

The coordination of research activities between the European Commission and the EDA has evolved against the background of a **wider policy** to protect the EU from the hazards that might arise from CBRNE – mainly framed by the EU Action Plans for CBRN and explosives respectively and complemented by the EDA's Capability Development Plan. The European Framework Cooperation (EFC) was established in 2011 when both institutions agreed to coordinate their research activities.

Under the EFC, **CBRNE was identified as a pilot case**, in which to explore dual-use synergies especially in the fields of detection, protection and decontamination between the FP7 Security Research programme and the EDA Joint Investment Programme for CBRNE.

In total, **73 projects** have been conducted at EU level in the area of CBRNE. Of these, 62 were funded through FP7 (2007-14), while the EDA oversaw the remainder through a Joint Investment Programme for CBRNE (JIP CBRN) (2012-), in which Member States have funded 11 research and development projects. Three years into this pilot, the cooperation on CBRNE research has developed at three levels:

- **The management of programmes** – The European Commission and EDA are participating to respective programme management committee meetings[62] They regularly exchange information on on-going and future activities, e.g. programme priorities, the results achieved from research;
- **The evaluation of proposals** – Experts from the EC and EDA have been participating as evaluators in the respective proposal evaluation processes;
- **The implementation of projects** – EDA representatives are participating in the advisory boards of three FP7 projects, and in the workshops, conferences, panels and demonstrations of another four[63]. Similarly, the EC has participated to the Executive Management Groups of JIP CBRNE projects and to expert meetings.

These cross-activities have fostered communication between the organisations and provided opportunities for insight into the activities of the respective initiatives, enabling better **coordination of strategies and solutions** to common threats by: promoting civ-mil R&D cooperation between the parties; coordinating projects to avoid duplication and to find coherence; and maximising complementarity among civilian- and defence-related security.

Project **dissemination** played a central role in the FP7 Security Research programme, and the results of CBRNE research were disseminated at both project and programme levels. Particularly noteworthy is the Community of Users on Disaster Risk and Crisis Management, which was established by the European Commission, and which also brought together participants from all projects in the CBRNE and crisis management fields.[64]

Therefore, within the limits imposed by legislation, the EC and the EDA have established a communication and cooperation channel that provides a good first step in the direction of tackling common threats and risks in a coherent and coordinated way, with the overall objective of ensuring citizens' security. Some stakeholders consulted for this case believe that this should be built on further during **Horizon 2020**, with involvement in a greater number of relevant projects and activities.

---

that is tackled by both military and civilian operators, and both sectors are developing products and solutions to counteract such threats.

[62] The SEC Programme Committee (FP7) and EDA Management Committee.

[63] As a member of the Advisory Board of the EDEN (the largest demonstration project on CBRNE), IFREACT and MIRACLE projects, and closely following other CBRN projects such as CATO, EQUATOX etc.

[64] For more details see the case study 3 on shaping the end-user landscape in the EU in Appendix F.

E.5 The FP7 Security Research Actions' impact on the competitiveness of the European security industry

The objective of **this case study** is to assess the extent to which the FP7 Security Research Actions have contributed to an improvement of EU competitiveness and of the European Security Industrial Policy. The case includes an examination of four projects that have been coordinated by private companies, in order to understand their approach to improving market competitiveness. Thus, it contributes to the evaluation of programme effectiveness in terms of industrial policy and competitiveness.

The **Security market** has been recognised as having significant potential for growth and employment in Europe, but it also faces particular challenges in that it is a highly fragmented market with a fragile industrial base. This is driven and reinforced by weaknesses that include:

- An absence of standardisation among purchasing bodies;
- A lack of common approaches to security issues, policy and regulation;
- Low levels of EU cooperation and organisation within the security industry;
- Conservative attitudes towards adopting new technological solutions, leading to a slowdown in the take-up and implementation of novel innovation .

One of the objectives of the **FP7 Security Research** programme was to increase the competitiveness of the European industrial security sector, including by tackling issues of fragmentation through projects relating to e.g. end-users, standardisation and interoperability. Despite a very high participation rate from Private for Profit Organisations (excluding education) (PRC) in the FP7 Security programme, its contribution to competitiveness did not always meet the expectations of companies – at least in terms of the direct uptake and exploitation of the project outputs (products).

The main areas of concern relate to programme structure and implementation, and include:

- **The lack of commercialisation**. Projects funded under the Security theme focused more on technological development than the commercialisation of the outputs and their operational use. However, it is worth noting that this is not specific to the Security theme, and in part reflects the relatively short timeframe of FP projects more generally (which may be insufficient to undertake both research and innovation work and then commercialisation activities);
- **The low take-up of results**. Low levels of cooperation between end-users and commercial companies have led to final results that are not well aligned with demand and / or are not sufficiently market ready;
- **The lengthy FP process**. The time from initial definition of work programmes to project completion and exploitation of outputs can reduce the eventual relevance of project results;
- **Complex IPR rules** can inhibit products being developed from project results;
- **Different national standards** are applied, resulting in high market fragmentation.

However, it is worth noting that knowledge, cooperation and networking benefits are widespread, and are seen as equally important assets for competitiveness – though their impact may only materialise in the longer term.

Some of the **projects led by PRCs** and implemented under the FP7 Security Research theme have tried to tackle the issues listed above by adopting different approaches. These projects suggest that the priorities for increasing competitiveness from the point of view of commercial companies are:

- Strong interaction with end-users, increasing the marketability of final products;
- A strong commercial component in the membership of consortia;
- The enhancement of the security supply chain (as a project objective), in order to improve the way in which companies operate;

- SME involvement in the programme, considering their higher flexibility and ability to respond to short-term capability gaps;
- Standardisation of procurement procedures and requirements, to reduce market fragmentation;

The experience from the FP7 Security Research Actions suggests several fundamental steps should be taken in **the future** in order to increase the positive impact of Horizon 2020 on the competitiveness of the market. In particular, actions under H2020 should be further focused on strengthening common approaches and standards. In addition, more focus, both at the programme and project level, should be given to the marketability of the results of the projects. Related to this, closer cooperation between end-users and the research and commercial communities is of strategic importance, and more emphasis should be placed on networking and understanding end-users' operational needs, even at the project proposal stage.

E.6 Productive Use of IPR from Security Research Actions

This case study considers the use of Intellectual Property Rights (IPR) within the FP7 Security Research programme, and focuses particularly on the achievements and experiences of a small number of research projects that have specifically led to IPR as an output. Looking at the potential use and dissemination of results through IPR, the case study contributes to the evaluation of the effectiveness of the programme with respect to the development of the security market.

IPR are the rights to use and sell creations of the mind, and cover such things as patents, utility models and industrial designs. IPR systems play an important role in the innovation process, protecting the investments of innovative players and serving as a key incentive to undertaking risky investments. They are also important for the dissemination and exploitation of research results.

Promoting the **use and dissemination of results** of FP projects was a key objective of FP7, and participants in the Security Research programme (as elsewhere in the Framework Programme) have been strongly encouraged to consider and tackle IPR issues as soon as possible during the preparation of their projects. The European Commission has also been committed to improving IPR management in research projects, and has attempted to clarify and simplify IPR provisions compared with FP6 (e.g. through a guide to IP rules and an IPR helpdesk).

Security research though, is considered a special case, as it often involves classified data and information, or sensitive results. As such, specific rules have been established to govern the use of IPR in this field – with the transfer of foregrounds to third parties continuing to be decided on a case-by-case basis, and with the greatest of caution.

From the initial tranche of 61 completed and assessed Security projects[65], only 7 (11%) are known to have **resulted in IPR**, generating 9 patent applications, 1 copyright and 1 utility model between them. This suggests that only a small proportion of all Security projects will generate and report IPR by the time of their completion - possibly some 30-40 projects, and 50-60 IPRs. Compared to the Cooperation Specific Programme overall (19%)[66], this is **relatively low**, which is perhaps surprising given the largely applied, near-term nature of much of the Security Research programme. However, the comparably low level of exploitation and patents for FP7 Security Research may be a result of the strategy to focus the SRAs more on integration than on the technologies needed for security applications that may exist already.

[65] As of the end of December 2014.

[66] Calculated from data presented in the FP7 Monitoring Report 2013, based on final reports submitted and assessed as of 1 December 2014.

Another possible explanation is that the security industry tends to protect results, at least in the short term, by **means other than IPR**. Even if results are expected to eventually find commercial application, this will often require additional time, effort and investment – and the relatively high cost of maintaining IPR, means that project partners might not immediately rush to address IPR protection.

Often projects will result in proven concepts, rather than marketable products, and **further steps** and additional investments are needed before results can be marketed. For instance, even though the SECRICOM project successfully achieved a proof of concept, the prototype was not ready for application immediately after the project. However, the knowledge and IP generated have been feeding into another FP7 project (FREESIC). A comparable situation exists for project EMPHASIS that took off from the LOTUS project, both complemented by project BONAS.

The **dispersal of IP** across consortia, and a lack of central control and awareness of outcomes, may also be reducing the generation of IPR, or at least the extent to which it is reported to the Commission. Most of the time foregrounds are generated and owned by individual partners, who can then make use of, protect and exploit this IP as they wish. For example, the SECRICOM project allowed at least five partners to develop new products, yet only one partner has so far patented their outputs. Often partners are not aware of IPR activities conducted by others, and IPR in the project final report, may only represent a proportion of the real situation.

In addition, feedback from the consulted projects suggests that IPR is often seen as too **complex and costly** to tackle, particularly amongst academic partners, who often do not have dedicated and competent staff in this area. Others lack the knowledge, skills and experience to address questions of IPR management. There can also be a mismatch between the interests of different project partners – and particularly between academia and industry – as well as competition between the industrial partners. A lack of professional management of IPR can also dissuade industry from participating in collaborative research projects, as well as cause potential conflicts during the projects and the limited application of results.

Those interviewed suggest that for a project to result in the production of IPR, a number of **conditions** are important. These include:

- Knowledge transfer and IPR management being clearly defined, with procedures and rules set out before a project starts;
- IPR possibilities being assessed at an early stage so that successful marketing can occur, and a clear and strategic structure to handle IP can be put in place;
- The development of structures and commercialisation plans that distinguish between dissemination of findings and application of the results;
- The devotion of sufficient time and resource to dissemination and exploitation;
- The inclusion of industrial partners within consortia.

While general **guidance** has been produced on IP issues for project consortia, reaching an agreement on IP sharing arrangements can still be complicated. A more extensive awareness and understanding of the importance and management of IPR issues among partners is felt to be important. Initiatives such as the Commission Guide to Intellectual Property Rules for FP7 Projects should be repeated in order to promote a better awareness of IPR issues. The role of the European IPR Helpdesk to provide participants with clear advice in relation to IPR should also be reinforced. Professional management of IPR issues within individual consortia might also be addressed through the association and support of various patent agencies.

E.7 Demonstration projects

This case considers the role of demonstration projects within the FP7 Security Research programme and explores the extent to which they have been successfully deployed to promote the application of innovative security solutions. It contributes to the evaluation of the achievements and European added value of the programme.

Technology-oriented research in the FP7 Security theme consisted of several **building blocks**, representing three routes that contribute to the overall mission objectives. On the top level of this structure were demonstration projects, which were intended to carry out research aimed at the large-scale integration, validation and demonstration of new security systems of systems, going significantly beyond the state of the art.

From the first (2007) work programme of the FP7 Security Research Actions it was stressed that the successful demonstration of novel solutions would be a key factor for the take-up and implementation of research outputs. The important role of demonstration projects, as **flagships** of the Security theme was therefore highlighted.

Following the advice of the high-level working group European Security Research Advisory Board (ESRAB), the Security Research programme implemented the demonstration programmes in **two phases**, whereby a series of initial support activities were used to define strategic roadmaps and increase awareness, in preparation for a smaller number of full demonstration activities.

As such, the programme initially funded a series of nine short pre-demonstration actions (**Phase I projects**) in five selected areas of significant European interest. These projects are all now complete and, according to the stakeholders consulted, they were successful in achieving their objectives, e.g. to build common understanding of key concepts and to clarify the notion of "system of systems".

However, even though these projects are generally considered to have met their objectives, their deployment has not been without **issue**. In particular, stakeholders were concerned that the short duration of these projects did not allow sufficient time to provide the comprehensive analysis of existing solutions that was required, or to properly engage with end-user communities. Their deployment in the early stages of the FP7 Security Research programme also meant they could not benefit fully from the outputs of many of the FP7-funded capacity and integrated projects. However, longer Phase I projects, or later deployment, would not have allowed sufficient time for the Phase II demonstration to take place within the seven-year period of FP7.

Five **Phase II projects** were then launched off the back of these preliminary actions, to deliver the system of systems demonstrations in each area. Among the five projects, only one had finished (SECUR-ED) and another was near completion (PERSEUS) at the time of writing. The three remaining Phase II projects were all still in the process of delivering their main demonstration phases. The two (near) completed projects are considered by the stakeholders consulted to have been successful in experimenting with the integration of different solutions in "real-life situations". However, it was too early to know what the impacts of these projects would be on the relevant security issues that they sought to address.

Stakeholders have identified several **potential issues** in relation to Phase II projects. The fragmented EU end-user landscape is thought likely to prove a barrier to the adoption of EU-wide solutions, and further efforts may be needed to move from the successful demonstration of solutions, to their widespread adoption. Also, it was highlighted that the actual buyers of the solutions demonstrated are not necessarily the same people and organisations as the end-users that are participating in and engaged with the demonstration activities. This may also limit widespread adoption.

Given that demonstration projects were intended to identify the 'real life' challenges of a system of systems, and to promote the application of innovative security solutions, individual projects in both phases were required to have significant involvement of **industrial partners and end-users**. Three of the Phase I projects had no end-user or industrial partners directly participating within their consortiums (to avoid choosing one solution over another for business reasons only). However, all first phase projects employed activities relating to the engagement of end-users. End-users (in larger numbers) have similar roles in the second phase projects, as well as direct participation in the demonstration activities themselves. In addition to single end-users, several projects involve end-user umbrella organisations within their consortia.

Several suggestions are made in relation to demonstration activities in **the future**:

- To maximise the benefits of end-user involvement – it is important to ensure very early involvement of relevant actors in the definition phase of projects (both in Phase I and early Phase II projects). This can be supported through end-user project coordination and the participation of umbrella organisations in consortia;
- To increase awareness around a project – it is suggested that communities of interest are established, particularly where these communities are small and well defined. Umbrella organisations can also play an important role as intermediaries;
- To increase the potential impacts of projects - it is important to clarify whether or not end-users are also potential clients / buyers for the solution. If not, partners should seek the integration of final clients in the consortium as well;
- To ensure cross-EU applicability - non-technical issues (e.g. different legal frameworks and national specificities) should be taken into account in the text of calls for proposals, as well as in both phases of demonstration projects, especially when tackling cross-border issues and broad areas of policy.

Finally, the scale and scope of demonstration projects should be flexible, in order to best suit the different cultural, legal, ethical and technological issues that exist in different areas. While some demonstration might be large and focus on developing EU-wide solutions, other areas might call for more modest demonstration activities and goals (e.g. where "system of systems" solutions are not yet appropriate).

E.8 Protecting critical infrastructures – Port Security

This case study explores how port infrastructure security was addressed through the FP7 Security Research Actions – both at a programme level, and through individual projects that have wholly or partially tackled the issue. Based on desk research and interviews with selected participants, it considers the results of these activities, and draws conclusions and lessons for the future. The case contributes to the evaluation of programme effectiveness in improving security capabilities and reducing gaps.

Ports are very important to the EU economy, and were identified by the Commission in 2004 as one of several **critical infrastructures** in Europe. A successful attack against a port has the potential to cause mass casualties, extensive damage and major economic disruption. Therefore, ensuring effective port security has become essential for the economic wellbeing of the EU. However, modern ports face **multiple challenges** and a far wider **range of threats** than has been the case historically, requiring comprehensive and reliable security solutions. Moreover, ports are nodes where highly complex systems of freight and passenger transportation interact and where a multitude of private but also public actors need to collaborate closely to ensure a smooth functioning of processes. Both aspects call for a systematic approach to security that ensures interoperability between systems and across all actors. The European Security Research Advisory Board (ESRAB) identified port security as an area of strategic interest for security research, and one which fell within the scope of two missions area ('Border Security' and 'Critical Infrastructure Protection'.

The FP7 Security Research Actions have addressed the specific requirements of **port security** through the different 'research routes':

- The Work Programmes of 2007 and 2009 included calls for **integration projects** that related to 'main port area security systems'. The SUPPORT project was funded with the participation of a broad range of actors, not least a number of European ports;
- In the final years of the programme, and in light of the then on-going project SUPPORT, port security was not explicitly addressed anymore but was tackled as part of a wider research agenda on maritime security. In this period, additional integration projects and in particular a **demonstration project** – PERSEUS – were funded.

Within the FP7 Security **project portfolio**, eleven projects have been identified that address port security issues to some degree (determined from the text of project abstracts). Reflecting the assessment of the Work Programmes above, most of these projects originated in the earlier part of the Security Research programme.

These projects with a 'port security dimension' involved over **243 organisations**, including the direct participation of at least one port authority in four cases. Indeed, **end-users** have been actively involved in all stages of the projects considered, and have provided essential user insight to product and system development.

Only one project (**SUPPORT** – Security Upgrade for PORTs) was exclusively focused on the issue of port security. In line with the Work Programme, the project recognised the importance of port security for Europe, as well as the challenges faced in improving port security, due to the complex operational modalities and lack of efficient organisational and technological interfaces between the actors concerned. It therefore sought to address 'total' port security solutions - encompassing legal, organisational, technological, training and human aspects – that would also integrate legacy port systems with new surveillance and information management systems.

Starting from the perspective of its partners' port operations, the project was able to identify major security gaps, and produce generic port security models that describe security measures to maintain or increase the level of efficiency and safety of these ports. The key output was the **Port Security Management System** (PSMS), which provides information, skills and methodologies to enable Port Facility Security Officers (PFSOs) to maintain, evaluate and upgrade their security measures and create security awareness, and thereby provide substantial improvements in the performance, reliability, speed and cost of European port security. The solutions were demonstrated in several EU ports (Gothenburg, Lisbon and Piraeus) and have already been purchased by the Port of Dublin, which was not a partner in the project.

Other projects identified as having a 'port security dimension' were not specifically and solely dedicated to port security issues; they included components relating to port security, but only as part of a broader set of issues being tackled. Many of these projects have led to the development of improved technologies. For instance, the UNCOSS project, which aimed to develop detection systems to identify weapons sitting on the seabed, succeeded in providing a fundamental technology for the global issue of maritime surveillance and ports / naval infrastructure protection, with the production of a prototype of a complete coastal survey system. Other projects led to field demonstrations of proofs of concept and prototypes. For instance, the SECTRONIC project resulted in field trials of 13 security scenarios, with sensors and communication equipment assessed through field evaluation against real targets. The SECTRONIC system was then developed and installed in ports (Rotterdam and La Spezia) for an operational evaluation period, and is considered to have performed well.

To conclude, several lessons from the experience of the projects studied in this case study might provide useful learning for **the future**.

- It appears that the demand-based R&D approach is beneficial, and can increase the impact and effectiveness of EU funding. It can also shorten time to market, because R&D is in line with end-users needs from the beginning, and because the participation of industrial companies ensures that results can be marketed soon after the end of the project.
- End-users, in particular public authorities, have played a key role in port security projects. They have assisted researchers in identifying gaps and vulnerabilities in protection systems.

Their involvement in the development process is seen as crucial, specifically during the testing phase; when matching the technology to operational realities; in drawing an appropriate scenario; when defining the application parameters; and in understanding the implementation process.

For H2020 the active involvement of end-users should be maintained and broadened. The Commission should explore ways to build on the experience of these projects with regard to end-user involvement and to transfer the lessons learned to other (mission) areas where end-user involvement has remained a challenge.

E.9 Tools, methods & resources to restore safety and security in case of crisis

This case study explores FP7 Security Research projects dedicated to the development of common methods, tools and resources to restore safety and security in the case of crisis. It examines the results of these activities and the impact they have had on cooperation capabilities between Member-States. The case contributes to the evaluation of the European Added Value (EAV) of the Security Research Actions, as compared to initiatives undertaken by the Member States individually.

In its 2006 report, the European Security Research Advisory Board (ESRAB) recognised an increasing need for **new and innovative solutions** (tools, infrastructures, procedures and resources) that would allow for greater cooperation between Member States and more efficient and effective response and recovery in relation to crises. In response, the FP7 Security Research programme was established with 'restoring security and safety in case of crisis' as one of four main thematic mission areas. One of two main challenges to be addressed by projects in this area was to improve the tools, infrastructures, procedures and organisational frameworks to respond and recover more efficiently and effectively both *during* and *after* an incident.

In total, 55 projects were funded through the **restoring security and safety in case of crisis** mission area (as of December 2014). From the project abstracts, it would appear that the majority of these focused on the development of methods, tools and resources, and among these it is possible to identify three main clusters:

- Projects with a clear focus on developing a common EU solution;
- Projects with a clear focus on developing a specific tool/method, with the intention of fostering interoperability or cooperation;
- Projects with a focus on a specific tool/method that include activities related to the potential cooperative use.

However, whilst most projects in the selection explicitly address (according to their project abstracts) interoperability and cooperation between different actors (cross-organisational working), only a small number explicitly focus on interoperability and cooperation between countries (**cross-border working**). For example: the FAST-ID project sought to develop an information management and decision support system to facilitate information sharing and cooperative planning across nations in relation to disaster victim identification; the PRACTICE project sought to create a system that would provide Member States with a flexible and integrated system for coordinated response to CBRN terrorist attack; and the FORTRESS project sought to develop an incident evolution tool with cross-border capabilities.

The projects have different ambitions in terms of the **tools and methods** they set out to design and develop. Several focus on the development of online platforms and interoperability systems for communication and data exchange (e.g. IDIRA, IMPRESS). Another group deals with the development of specific individual tools and resources for detection and protection (e.g. INDIGO, IF-REACT). Some of the projects focus on the development of toolboxes, which gathering and integrating different tools, methods and guidelines, to support decision making (e.g. CATO, PRACTICE).

Most of the projects involve **end-user** organisations (commonly emergency services and public security services) directly in their consortium, while two projects are led by end-users. End-users are also commonly engaged during projects through interviews, workshops and demonstration activities. This has been important in identifying end-user needs, defining requirements and collecting early feedback on outputs. The involvement of end-users is also thought to have been useful in reducing the time-to-market of final outputs, and in raising awareness of project activities and results.

Only half of the selected projects were due to have completed at the time of writing, meaning evidence on **outputs** and impacts is only partial. However, stakeholders consulted for this case believe that most projects have already been successful in achieving at least part of their goals. Examples already available of project achievements include: prototypes for interoperability systems, decision-making support tools and tools for first responders (e.g. FAST-ID); toolboxes, technological frameworks and guidelines (e.g. CATO); and standard-related activities (e.g. CATO). However, projects are often not intended to result in market-ready products within the timeframe of EC-funded activities, and it will be down to individual project partners to work on the outputs further once the projects have concluded.

Stakeholders consulted for this case have identified several **challenges** that can reduce the potential impacts of the projects under examination. In particular, even though most projects engage with end-users and policy-makers in one way or another, the timing and channels used are not always the most appropriate. Also cooperation between different end-users can prove difficult because of their different cultures and expectations, and their often-limited experience of participation in R&D projects.

The analysis and feedback suggests that **future efforts** to develop tools, methods and resources to restore safety and security in case of crisis would benefit from better-organised communities of relevant users, increased dialogue and interaction between related projects, and greater involvement of end-users in the projects themselves.

E.10 The involvement of the citizen in security research

The focus of **this case study** is the involvement of citizens in FP7 Security Research. It considers the extent to which citizens genuinely participated in the FP7 Security Research Actions and in what kinds of projects. It reflects upon the purpose of the involvement of citizens, if there were any gaps, what the challenges of engaging with citizens are and how they are overcome. In addition, it addresses the impact and advantages according to project participants and explores how project results were disseminated and whether they reached relevant communities. The case contributes to the evaluation of effectiveness in terms of reaching intended target groups and the potential impact and added value from citizen involvement.

More than other research themes security depends on the acceptance or tolerance of research results by citizens. Security of the citizen includes the protection of the citizen, but, to be effective, also encompasses issues such as privacy, dignity and liberty of individuals. The case examines the **engagement of citizens**. The definition of citizen engagement i.e. of the different ways in which citizens might become involved in security research projects is quite a complex issue. This case focuses on individual citizens rather than citizens as representatives of organisations, although some consideration of Civil Society Organisations (CSOs) is also made.[67]

The issue of citizen engagement with the Security Research Actions is important, as there has been some critique of the **poor record of citizen engagement** within the European Security Research Actions (SRA). For example, in 2011 State Watch complained that the EU security research agenda has been strongly influenced by the representatives of corporations from the

[67] Representatives of CSO, as well as researchers are citizens too. However, their participation in research projects is based (legitimized) on their organisational membership and expertise (functional roles) and not the mere fact that they are citizens. Moreover, it can be assumed that their motivation is *primarily* guided by their functional roles rather than by a concern for the public, which is not to say that researcher and CSO representatives are not concerned about the public weal, just that their functional roles take precedence or are at least an additional factor when it comes to matters of motivation and judgement. A citizen is assumed to be responsible only to her consciousness.

defence and security industries[68]. In 2014 a report by the European Parliament also commented that security research had only partly addressed the concerns of EU citizens and that security research has been mainly aimed at the service of industry rather than society[69].

The results of this case study suggest that **citizens are under-represented** in the FP7 Security Research programme. This point is equally made in the academic literature, the interim evaluation of the FP7 Security Research Actions,[70] as well as several reports from CSOs. At the project level, the engagement of citizens and CSOs is rather limited and is not really contributing to shaping the technologies being developed. Moreover, citizens are engaged in FP7 Security Research Actions predominantly as an object of research and to a much lesser extent as active research subjects.[71] Interviewees from research projects speak positively about the results of engaging with citizens, but questions remain about the extent of actual involvement, the quality of the engagement and the practicalities of genuinely including citizens and their views in the security actions.

In **conclusion**, there is some positive degree of citizen engagement in the security research programmes but importantly this is quite limited and is not really contributing to shaping the technologies being developed. It is an engagement that happens mostly post hoc, i.e. after the research design is in place and after the results have emerged. Consequently, the case study suggests that some up streaming of citizen engagement at both, project and programme levels may be beneficial for the future.

Specifically, the following **recommendations** are offered for future programmes:

- The Commission should encourage security research projects to engage with citizens. A priority would be to consider carefully whether a topic of the work programme would benefit from direct citizen participation and if so, to include it in the requirements and the evaluation criteria;
- The case has pointed to a number of practical mechanisms used effectively for citizen engagement by projects such as interviews or focus group workshops with citizen where input is gathered or preliminary project results, issues or concerns are systematically discussed; or the involvement of volunteers to contribute personal data, thereby helping to construct a temporary databases. In any case, these mechanisms should be collated systematically and made available for project applicants to draw upon. This should be further broadened by a more in-depth study on this topic, to be made available to security research action applicants in order to facilitate their projects;
- Furthermore, the Commission should investigate ways to involve citizens at programme level, for example in shaping the work programme, in reviewing projects, or at the dissemination stage, e.g. through citizen's panels.

Finally, this case study has yielded a range of **emergent considerations** around the topic of citizen engagement in security research, which should be examined in a more extensive manner, when going forward. These concern in particular whether more citizens should be directly engaged in the work programme for the new framework for security research, and - if this is deemed desirable - then how to engage the citizens. Questions could be: Should projects themselves all be encouraged to have a strong component of citizen consultation? Should separate research projects consider citizen views on relevant societal related consequences of technologies or should the Commission run citizen focus groups to consider the new ideas, products and processes emergent from the research projects and wider citizen consultations to shape the work programme itself?

[68] Statewatch (2011) Rethinking the EU Security Research programme.

[69] European Parliament (2014) Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013. Study PE 509.979. Brussels.

[70] CSES (2011) Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research. Sevenoaks.

[71] In this context please note the remark on the fact that representatives of CSOs and researchers are citizens too, made above in footnote 67.

E.11 Project clusters – success factors for cross-project collaboration

Across the Framework Programme there are a number of examples of **project clusters** that have emerged around particular topics or challenges. These have sought to exploit synergies between related projects and achieve greater impact through networking, coordination and other joint-activities.

This case study examines the activities and experiences of the first clustering of projects in the FP7 Security Research programme, which involved three projects focussed on different aspects of the subject of surveillance, which was established between the FP7 Security and Socio-economic Sciences and Humanities (SSH) themes. It illustrates how cross-project collaboration and coordination can be approached, and highlights some of the benefits, as well as the challenges, that can result from such efforts. It contributes to the evaluation of the efficiency of the implementation of research projects and the effectiveness of the dissemination of results.

The Commission initiated a coordinated approach having identified that surveillance would be relevant to both the SSH and Security Research programmes, and that there would likely be complementarities between projects funded. A **coordinated call** was issued in 2011, with the subsequent proposal evaluation processes also conducted in parallel. This resulted in the selection of three projects (RESPECT, SURVEILLE, IRISS), each addressing surveillance from a different perspective, and covering socio-cultural, legal, ethical, technical and operational elements.

The **aim** of the joint call and subsequent project cluster[72] was to bring together experts from different disciplines to look at surveillance from different angles, and to provide an opportunity for them to engage and test their ideas against each other. It was hoped that this would lead to more comprehensive results and relevant recommendations. The initiative also functioned as an experiment in the use of joint calls and resulting coordinated activities, intended to inform the EC's thinking about similar approaches in the future.

The Commission organised an initial meeting with the three project coordinators, where also the **joint activities** required of the projects were explained (including: sharing deliverables; attendance at each other's meetings; a joint event; and a joint policy document). The three projects formed a joint platform called DEMOSEC.

Each of the requested specific joint activities was undertaken by the projects. However, overall, collaborative activities remained a marginal aspect of the projects, and the benefits and impacts of the cluster were quite limited as a result.

There is some evidence of **cross-learning** between the projects, with greater awareness of the activities of the other projects, and some efforts to build-on others' work during the course of the research. However, such activities were limited, and some partners saw scope for greater levels of joint-working and collaboration.

Experts interviewed for the purpose of the case study found the **joint conference** as the only real significant joint activity that took place as part of the cluster initiative. The project representatives were generally satisfied with this event, and suggested that their project was able to achieve greater visibility, reach a larger audience, have more interesting discussions, and integrate a greater range of perspectives than would have been the case had they just held individual end-of-project events. However, the organisation of this joint event was considered something of a challenge by all of the project representatives consulted, and it was not obvious whether the additional cost and effort required was justified by the additional value gained from hosting the event together.

In conclusion, it is not clear whether the cluster fell short of expectations, because these are not explicitly set out, and (as a result) because views on what should have been achieved vary between the different individuals that have been consulted.

[72] The 2011 Work Programme referred to 'a coordination' with the corresponding SSH topic – the term 'cluster' was only introduced, more informally, when the projects started.

This was a first attempt at creating a simple project cluster within the Security Research programme, and the projects did indeed fulfil the specific requirements in terms of joint activities, which brought some benefits. However, some of the project partners had expected greater cross-project collaboration, and there was some expectation on the Commission side to see the project coordinators use the initiative as a platform to further develop research collaboration beyond the minimum requirements – something which did not occur.

It has been suggested by project representatives that the cluster idea was introduced too late in the project planning process (and without specifically allocated funding) for cooperation to be embedded meaningfully into the respective research plans and activities. There was also a lack of clarity as to the scope and purpose of the initiative, with a lack of communication between the Commission and project coordinators, and between the coordinators and wider project teams. The projects (through their coordinators) do not seem to have bought-in fully to the cluster idea, and tended to see the collaboration as a top-down additional requirement, rather than an opportunity.

In **the future**, if the clustering approach is to seek more substantial research collaboration, project representatives suggested: (i) to identify and focus efforts on specific topics of shared interest (and not try to collaborate on everything covered by the various projects); on those topics, organising work packages or targeted events would ensure genuine collaboration; and (ii) to provide additional funding earmarked for collaboration, similar to network funding to cover transaction costs used in other areas. Collaboration takes time and resources, and projects are reluctant to engage if it means reallocating resources away from already planned research activities.

E.12 Participation of smaller EU countries in FP7 Security Research Actions

The aim of **this case study** is to investigate the participation of smaller EU countries in the FP7 Security Research Actions. As one might expect, smaller countries have participated less in the Security Research programme than larger countries in absolute terms. Looking at participation data in relative terms, however, shows that a number of smaller countries have performed well, considering their size, GDP and overall FP7 participation levels. The case contributes to the evaluation of the Security Research programme's attractiveness to actors in smaller Member States and its complementarity with other initiatives in these countries.

Four examples of such countries – Luxembourg, Slovakia, Latvia and Estonia – were studied in more detail, through desk research, analysis of CORDA data, and interviews with a selection of relevant experts.

The participation rates of Luxembourg and Estonia were well above EU average in relation to their size, whereas Slovakia and Latvia participated at a rate similar to the EU average. For all four countries, however, participation in the FP7 Security Research programme was much higher as a share of total participation in the Cooperation Specific Programme than the EU average – and in some cases twice the rate.

Latvia had a very high rate of participation from Public Bodies (excluding research and education) (PUB), whereas the three other countries considered tended to draw a majority of participants from Private for Profit Organisations (excluding education) (PRC) and Higher or Secondary Education Organisations (HES).

All four countries reported a relative absence of large companies and a preponderance of SMEs. This informs their approach to supporting participation in EU programmes.

Different avenues were explored through the case to try to explain the **reasons behind (relatively) high levels of participation**. The main factors were:

- The existence of national strategies and programmes for security research;
- Leading actors (often just one or two) driving national participation;
- The sense that in smaller countries 'everyone knows each other';
- Support to (potential) participants (e.g. through the NCP or funding).

Correspondents in the four countries gave several **examples of good practice** that had helped the NCPs to play an effective role. These related to:

- The organisation of the NCP function (the choice of host institution and stability in individual NCPs for the security theme over time);
- Taking advantage of existing networks to engage with stakeholders;
- Providing relevant information for new applicants, and 'customised' engagement with SMEs.

There was relative consensus in the four countries about the **main benefits** of participating in the FP7 Security Research programme. Accessing funding was seen as important, but other factors were also important (often more important) drivers. These included benefits relating to networking, collaborating on shared problems, additional funding for innovation, and the specific outputs of projects.

It was generally expected, that for these smaller countries, participation rates in Horizon 2020 would be similar to that seen in FP7. There was, however, a set of commonly agreed **barriers** that still persist. These revolved around:

- Convincing inexperienced, small and locally-focused actors to participate;
- The seeming tendency towards larger projects, which can prove more difficult for small countries to participate in or coordinate;
- Engaging public sector end-users, who have been under-represented participants.

The findings of the case study point towards actions that could be taken at national and European level to help strengthen the participation of smaller Member States in Horizon 2020 and in **future security research programmes**.

One of the key strengths identified across the four countries has been the effective internal coordination. In some cases this was informal, but there were also several examples of how the support system was effectively set up to exploit existing networks and to ease access to stakeholders. Even larger Member States could draw inspiration from these examples to improve their national systems.

In all the countries studied here, SMEs were seen as the most important constituency, and frustration was expressed over the barriers these organisations faced in participating effectively in European projects. In particular, concerns were raised about the tendency towards larger projects and consortia, without open competition, which was considered not to favour smaller organisations.

Many newer Member States are comparably small and it was suggested that additional support from the Commission in the form of practical guidance and more frequent visits to these countries might help NCPs be more effective.

Finally, several countries reported that PUB organisations that could benefit from participating were constrained by internal rules and regulations. Reforms will be needed to facilitate future participation from this important group of end-users.

E.13 Dealing with challenges in diverse project settings involving numerous types of partners

This case study considers the difficulties involved in managing research projects with partners from diverse backgrounds, and explores examples of these challenges and the approaches taken to address them within specific FP7 Security projects. It contributes to the evaluation of the efficiency of the management and implementation of FP7 Security Research Actions.

Project coordinators face numerous practical difficulties in the context of the **management of large and diverse teams**. The projects in the FP7 Security Research theme involve not only partners from different disciplinary backgrounds, but also bring together participants from research, industry and end-user organisations.

On average, projects in the FP7 Security Research programme involved 12 different participating organisations (which is above average), and in most cases participants from three or all four of the main types of organisation (Higher or Secondary Education Organisations (HES), Private for Profit Organisations (excluding education; PRC), Public Bodies (excluding research and education; PUB) and Research Organisations (REC)).

The scale and shape of the project consortium for successful collaborative activity has been the subject of much previous research. Drawing on a small sample of interviews with Security Research programme participants, this case study elaborates some of the challenges of managing diverse project settings, involving different types of partners and identifies examples of good practice. The case focuses on three projects – CRISMA, SPEEDKITS and ESS - that involved various types of partners in large consortia, and explores the challenges they faced and how they were addressed.

The **main challenges** identified during the proposal and project stages include: achieving a shared vision; aligning/accommodating differing expectations, priorities and views; securing the appropriate skills and capabilities, and making best use of these; achieving a common language and means of communication; and dealing with IPR, confidentiality, security, ethics, and commercialisation issues before they arise.

The case study suggests that there may be an **optimum level** of scale and diversity in projects, beyond which both efficiency and benefits decline. In small scale, low diversity projects control is easy, but the critical mass for the generation of creativity and novelty may be lacking. Larger and more projects meanwhile may have significant capabilities and a wide range of interests, but these are also difficult to coordinate, and the costs of managing them in terms of time and effort may simply be too great. Indeed, the sheer scale may be so great and the diversity so large that agreement within the project is not possible.

From an examination of example projects, the case found **three key factors** to help managing successful diverse project settings, which may provide useful lessons for the future. These relate to ensuring a shared commitment, a common understanding, and a common language. In addition, effective team building and foresight by project managers, combined with effective communication tools, can help to mitigate challenges faced by research consortia.

It is important to emphasise that although there are many challenges to managing large diverse project teams and although translation across sectors is not easy, many project partners find the benefits are worthwhile and the impact of the project can be significantly enhanced through the diversity of the group.

E.14 The significance of standardisation for Security Research Actions

An essential feature of security market is that it is a **highly fragmented market**, lacking harmonised certification procedures and standards. In the various areas covered by the FP7 Security Research Actions, standards can be used to reduce market fragmentation and improve interoperability between national systems.

The objective of this case study is to assess whether **standardisation** is an important part of FP7 security research projects and how the programme has managed to contribute to reducing the fragmentation of the security market through the development of standards. The case puts more emphasis on projects that have involved standardisation organisations – as they seem to be key players in pushing for standards. It contributes to the evaluation of the programme's effectiveness in improving coherence and overcoming fragmentation.

In total, **83 projects** have been identified as having a direct or indirect link with standards (based on the word "standard" being mentioned in the project abstracts). However, the 'standard' dimension is mostly a minor subject in most of these research projects, which leads to very limited outputs on standards in most of these 83 projects.

This suggests two things:

- There seems to be a discrepancy between the push from public bodies (Mandate 487 issued by the European Commission to ask European Standardisation Organisations (ESOs) to develop roadmaps and standardisation strategies in the field of security) to work on standardisation and the actual involvement of industrial stakeholders in standardisation activities in research projects;
- The "standard" dimension in proposals is often limited and is not considered a priority for most of the consortia working on FP7 security research projects. Standardisation bodies consider that the number of projects with actual standardisation content is very limited.

Among these 83 projects, nine have benefited from the participation of **standardisation organisations**. Standardisation bodies engage in projects with specific roles:

- In prospective projects (i.e. projects that aim to identify needs in the field of research), the Standardisation bodies' participation aims at providing inputs on what can be a standardisation strategy in one specific area;
- In more common collaborative research projects, they provide expertise on the standards dimension of a project.

Only four out of these nine projects were completed by December 2014. These have led to different **outputs** in terms of standardisation: guidelines on a standardisation strategy, with the identification of priority areas and demand (or lack of) for specific standards, CEN Workshop Agreements, pre-standard works, etc. Moreover, the participation of standardisation organisations (and the dedication of other partners to work on the issue of standardisation) is an efficient way to raise awareness among all partners on the issue of standardisation, build a coherent standardisation strategy and to ensure the follow up of this activity, even after the end of the project.

In **conclusion**, for the majority of projects, the actual planned work on standards is limited, especially because there is no resource dedicated to the issue. Security Research Actions have however led to some interesting work in the area of standardisation, especially because projects have contributed to identifying gaps and needs for standards.

The only way to produce standards or standard-related outputs from a FP7 Security Research project is to dedicate time and budget to this issue, and this can be done efficiently by involving standardisation organisations as partners.

E.15 The influence of FP7 Security Research Actions on national research programmes

An important aspect of the evaluation of the FP7 Security Research Actions (SRA) concerns the European Added Value (EAV) of the programme. In the context of this case study, EAV is defined as a benefit that cannot reasonably be achieved by the actions of individual Member States or an alliance thereof. **This case study** contributes to the discussion of EAV by examining the character of national security research programmes and their relationship with the FP7 SRA. It looks in particular at programmes in Austria, France and Germany.

Based on analysis and interviews with national representatives, the case concludes that these national security research programmes are **well aligned** with the FP7 Security Research Actions. In particular:

- The programmes **focus** on the national needs of security research, formulated in line with their national priorities in the security area. While they have addressed a variety of security threats through the support of end-users, they also address the competitiveness of the security industry and, in two cases, the creation of new jobs. This orientation echoes important aspects of the FP7 SRA objectives;

- Anecdotal evidence points to the fact that national programmes have in some cases addressed short-term needs, compared to the longer-term perspective of the FP7 Security Research Actions. In other words the programmes at national level have **complemented** the actions at EU level;
- Similarly, there is anecdotal evidence that the experience, competence and results from projects funded by national programmes have been built upon in projects funded by the FP7 Security research programme. The latter providing also the opportunity to access larger markets;
- More generally the analysis suggests that the national security research programmes have contributed to the **strengthening of networking and cooperation** in the Member States and in the European Union.

Through the Programme Committee, Member States have shaped the contents of the FP7 Security Research Actions. Six countries in particular – including Austria, France and Germany, which are the focus of this case – have used an informal structure to actively contribute to the Commission's work, and to coordinate research efforts at national and European levels.

The analysis of national programmes suggests that there are three main **lessons** that might be learnt for Horizon 2020: the involvement of end-users in security research projects should be mandatory; societal needs should be a focus of projects; and the results of projects should be disseminated to larger groups of end-users.

Appendix F Case studies on security research

This Appendix presents a **compendium of the fifteen issues-based case studies.**

Based on the results of desk research, analysis of survey results and stakeholder interviews undertaken during the first phases of the study, a number of important **cross-cutting, horizontal and overarching issues or topics** relating to the FP7 Security Research Actions (SRA) were identified that appeared worthy of deeper exploration. Executive summaries of all case studies can be found in Appendix E.

The **presentation** of each case varies slightly, according to the particularities of the issue in focus. However, each is broadly structured into three parts: a beginning (introduction, background and / or context), middle (analysis of findings from data collection), and end (conclusions and lessons for the future).

F.1 Ethics in security research

This case study explores how ethics have been addressed through the FP7 Security Research Actions, at both a programme and project level, and what effect this has had. It examines the processes that have been put in place to identify and tackle potential ethical issues at the proposal stage, and looks at some of the specific mechanisms then employed by projects to address issues during implementation. It also considers in more detail a selection of projects dedicated to researching ethics and security. The case contributes to the evaluation of relevance and effectiveness, as well as the efficiency with which ethics procedures have been implemented.

The first section of the case study provides a brief introduction to the issue of ethics in security research. The subsequent two sections concern the programme level and analyse the general FP7 ethics review process and the specific procedure for FP7 Security Research Actions respectively, followed by a section analysing three projects specifically addressing ethical issues. The final section presents conclusions and lessons learned from the case.

The research carried out for this case study included documentary analysis and four interviews with experts from the European Commission and research projects.

F.1.1 Background to ethics in security research

Ethical considerations are important for any research activity, but are particularly pertinent to security research**,** where it is critical that the products, processes and systems developed for security protection adhere to ethical standards and will be socially acceptable. Security measures adopted in relation to e.g. counter-terrorism, surveillance and organised crime are often associated with a potential loss of privacy and questions regarding infringements on civil liberties and human rights. Other common ethical issues in the development of security technologies include data protection, mediation and conflict resolution. Finding a balance between respect for fundamental freedoms and security is a particularly challenging and inherently complex task.

Ethical considerations are important for good research practice, but they are also crucial for the **perception of citizens** as to the integrity and outcomes of security research. This has become increasingly important in the so-called post-Snowden era. Therefore, addressing ethical aspects in security research contributes to social legitimacy and ultimately citizens' acceptance of the project results.

Security research has in the past faced **criticism** from both politicians and the media for a lack of consideration of ethical issues in areas such as intrusive technologies. The FP7 programme in particular has been subject to criticism as regards potential conflicts of interest, with multi-nationals receiving programme funding[73]. It is alleged that these organisations, who often help shape the security research agenda, receive funding through the programme and are then able to sell the technologies and systems back to the governments who ultimately provided the funding in the first instance.

Further, a **2014 review** of security measures in FP7 for the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament[74] found that most projects funded in the Security Research theme during the first years of FP7 were strongly technologically driven, with little attention paid to political and societal issues. It also suggested that research on freedom and privacy in the context of security technologies had been a weak component within the programme. The report highlighted that few projects had reflected on the ethical, legal, political and social implications of security technologies, and concluded that ethical considerations were perceived as an afterthought, rather than an integral part of security research.

[73] Statewatch (2011) Rethinking the EU Security Research programme.

[74] European Parliament (2014) Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013. Study PE 509.979. Brussels.

Such concerns are likely to have contributed to efforts to focus more attention on encouraging ethical consideration within the projects funded through the programme, as well as the funding of a greater number of projects that focus directly on ethical issues. Both of these routes are explored further in this case.

F.1.2 The FP7 ethics review process

Reviewing research projects on ethical grounds is a **legal requirement** under FP7, and the rules for participation in the programme specifically state that a proposal that contravenes fundamental ethical principles shall not be selected, and may be excluded from the evaluation and selection procedures at any time. Ethics review is therefore an important part of the process of evaluating research proposals submitted across FP7, including in the Security Research programme, and is intended to ensure that all research activities are conducted in accordance with fundamental principles.

All applications pre-selected for funding that raise ethical issues (as determined by the scientific evaluators) are subject to a standard **ethics procedure**. This process is split into two stages:

- Firstly, all applications pre-selected for funding that raise ethical issues must undergo an **ethics screening** - which results in an ethics screening report that indicates whether a more in-depth ethics review is necessary. Ethics screening is the responsibility of the individual programmes receiving applications and is carried out by independent experts. The ethics screening report may also include recommendations for negotiations (even when no second stage is required).
- Where required, an **ethics review** is then undertaken - where an evaluation is made of all aspects of the design and methodology of the proposed activities that raise ethical concerns, resulting in an ethics review report. This review is undertaken by independent experts from a variety of scientific disciplines, who have a special expertise in ethics.

Certain types of proposal (e.g. those involving a research intervention on humans) are automatically submitted to ethics review. Particular attention is also paid to research involving children, research in developing countries and security-related research.

The ethics review itself looks at (i) the necessity of using certain methods to achieve objectives, and whether there are alternatives, and (ii) the benefit/burden balance of the project and its various impacts. The review process results in an **ethics review report**, which summarises the expert's opinion on the ethical soundness of the project proposal. Any recommendations and requirements put forward in the ethics review or ethics screening reports are taken into account in subsequent grant negotiations and can lead to **obligatory provisions** in the conduct of the research.

Examples of **issues raised** through the ethics review of FP7 Security Research programme applications in 2011 include:[75]

- A lack of specificity on potential ethical concerns for 'human data collection';
- Little is said about ethical issues connected to how social networking tools will be approached or used, who will be targeted, or how users will be involved;
- No reference to the threats that the collection and processing of data creates for members of minority and dissenting social groups;
- No elaboration of the steps that will be taken to protect the rights, liberty and dignity of marginalised groups, vulnerable populations and minorities.

[75] Karatzas, I. (2011) Ethics Review of FP7-SEC-2011 applications: Issues raised in the Ethics Review, (presentation).

Monitoring of ethical issues is included within the standard periodic reports that the Commission requires and during project reviews for all projects where recommendations or requirements were provided in either the ethics screening report or ethics review report. Some interviewees consulted for this case raised a concern with this process, suggesting that the Commission is mostly interested in compliance (i.e. ensuring reports are completed), rather than any necessary follow up on ethical issues reported.

However, as of 2008, proposals that undergo ethics review can also be flagged as requiring an **ethics audit**, which is designed to assist researchers in dealing with the ethics issues raised by their work and in taking necessary corrective measures.

The **2013 FP7 Monitoring Report** shows that 2,094 projects had undergone ethics review in total, representing ~10% of all FP7 projects funded during the 2007-13 period. None of these projects were stopped as a result of the review, although in 1,007 cases the proposals were found to have insufficient safeguards, and modifications were requested. In addition, 209 project proposals were flagged for ethics audit.

The FP7 ethics review process forms the basis for efforts across **all thematic areas** of the Cooperation Specific Programme. However, the extent to which projects go through this process varies, based on the degree to which ethical issues are relevant and significant considerations in the different programme areas. The remainder of this case considers the specific case of the FP7 Security Research programme.

F.1.3 The ethics review process in the FP7 Security Research programme

The FP7 **Security Research programme** has strengthened the attention given to societal issues, like privacy and ethical issues, during the course of FP7. This is partly a reflection of a more general push within the Commission, led by the responsible Services within the Directorate-General for Research and Innovation (DG RTD), but also reflects a particular effort by the FP7 Security Research Programme to encourage projects to take proper consideration of ethical issues.

Work programmes

The wording of requirements in **Security work programmes** has developed over time to reflect a stronger focus on considering ethical issues within the programme, and FP7 more generally. The first Security work programme (2007) merely stated that "ethical principles must always be taken into account". This was extended slightly in 2009 to "…taken into account in planning, decisions and funding". Then, from 2010, a fuller explanation of ethical review requirements became a standard feature, stating that "proposed activities shall be carried out in compliance with fundamental ethical principles. If ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity. In addition, the potential impact of the resulting technologies and activities on fundamental rights, ethical principles and societal values should be addressed as part of the proposed research."

Leaving aside for the moment the specific funding of projects in the field of ethics research (discussed further below), there is an increase over time (see the table below) in the number of topics in other parts of the Security work programmes making **specific reference to ethics** and ethical considerations in the call text (e.g. requesting that projects address or consider ethical challenges, or that they should result in improvements in terms of ethics). Even so, some individuals interviewed for this case have argued that when preparing calls for proposals the programme could better highlight and raise awareness of possible ethical challenges that might be associated with the requested research.

Table 39: Topic areas mentioning "ethics" in the wording of calls

Year	2007	2009	2010	2011	2012	2013	2007-13
Number of topic areas	1	1	4	7	6	16	**35**

Source: Work Programmes 2007-2013; excludes calls under the 'ethics and security' area

It is also worth noting that interview partners had some comments regarding the **'checklist' table** that is included within FP7 proposal templates, and which prospective consortia must use to identify potential ethical issues that the propose project activities and research processes might generate.

Some argued that the checklist table is a very important element in the proposal process, as it helps researchers to pay greater attention to the potential ethical issues that may have a bearing on the projects, leads to some useful reflections and may reshape things a little in terms of methodologies and work plans. At the same time, others believed that it serves little purpose and just adds further administrative burden. Some also suggested that the checklist is not sufficiently in-depth and that it may omit some very important ethical considerations. However, it would likely be difficult to create a detailed and specific checklist of all potential ethical issues that might apply across the programme, given the variable nature of individual projects.

Ethics reviews

According to FP7 monitoring reports[76], the Security Research programme had among the highest number of **ethical reviews** of all the Cooperation Specific Programme themes (behind only ICT and health). The following table shows the number of reviews conducted each year in the FP7 Security theme and suggests that there were at least 90 over the FP7 period. This equates to around one-quarter of all Security Research projects eventually funded, which is much higher than the 10% rate seen in FP7 overall.

Table 40: Number of Ethics Reviews in the Security Research theme, per year and total

Year	2009	2010	2011	2012	2013	2009-13
No of ethical Reviews	11	16	21	18	25	**91**

Data extracted from FP7 Monitoring Reports. Data by theme for 2007 and 2008 is not available.

As of December 2014, 102 Security research projects had submitted final reports and 61 of these had been processed, with all outputs recorded within the Commission's SESAM **project monitoring** database. This partial dataset, comprising projects from the earliest calls and those of shorter duration, nonetheless allows some insight into the wider set of 300+ projects funded through the programme.

The SESAM database includes details of the ethical issues reported by the completed projects in the context of their final reporting and the related 'Report on societal implication'. Just over half of the projects assessed are noted as having at least one ethical issue reported, with 60 ethical issues identified in total across these projects. The number and types of issues identified are shown in the table below.

Table 41: Number of processed Security research projects where ethical issues were identified

Ethical issue	Projects
RESEARCH ON HUMANS	23
project involves adult healthy volunteers	*13*
project involves Human data collection	*6*
project involves patients	*2*
project involves Human biological samples	*2*
DUAL USE	17
research having potential for terrorist abuse	*11*
research having direct military use	*6*
PRIVACY	13
project involves tracking the location or observation of people	*10*
project involves processing of genetic information or personal data	*3*
RESEARCH INVOLVING DEVELOPING COUNTRIES	6
project of benefit to local community (capacity building, access to education, etc.)	*6*
RESEARCH ON ANIMALS	1
project involves research on transgenic small laboratory animals	*1*
RESEARCH ON HUMAN EMBRYO/FOETUS	0
Total ethical issues identified	**60**

SESAM database (as of December 2014)

[76] For the monitoring reports see http://ec.europa.eu/research/evaluations/index_en.cfm?pg=fp7-monitoring.

Mechanisms and approaches to ethics in project implementation

Ethical issues or concerns may arise at two stages of a research action: in relation to the research process itself (including procedural and conceptual ethics), and then once the system, product or other outcome from the research has become operational.

Concentrating on the former, it is possible to discern different approaches that have been employed by FP7 Security Research projects to ensure that ethical issues are effectively dealt with throughout the research process. This includes:

- **Parallel ethical research** (e.g. SAFIRE, CPSI). This approach goes beyond the Commission's requirements and includes adding an ethics expert to the project. This ethicist works alongside the project team, reviewing and discussing choices as regards methodologies and tools, but also other areas of relevance to the research.
- **Ethical Advisory Board** (e.g. ALERT4ALL, SCIIMS, SAVASA). Many projects have established an Ethical Advisory Board (EAB) to identify, monitor and analyse ethical issues during project implementation. In the same vein as parallel ethical research, the EABs support projects by reviewing methodologies and research tools in order to foresee and tackle ethical problems arising.

By embedding these mechanisms into the project implementation and management process, a range of ethical problems can be mitigated and resolved. For example, in the project examples given above, the issues most commonly highlighted through these mechanisms have been around the potential misuse of products, e.g. the danger of technology being used for criminal activity or falling into the 'wrong hands'. Participants consulted for this case have argued that project outcomes are more likely to be ethically justifiable and acceptable as a result of these mechanisms. However, they also noted that they can prove costly, and may not be justifiable for all projects.

These mechanisms focus on both **procedural** and **conceptual ethics**. Procedural ethics considers ethical issues emerging from the research process itself, such as issues of informed consent, privacy and data protection. Conceptual ethics relate to ensuring that the research subject is of highest possible integrity and ethical standard. This relates mainly to choices on, for instance, who to interview or what should be the subject under examination. Some of the individuals interviewed for this case have noted that the Commission places a strong emphasis on procedural ethics, but gives less consideration to (and few guidelines for) tackling issues of conceptual ethics.

F.1.4 Security research projects directly addressing ethics

Within the 'security and society' domain of the Security Research programme, the issue of ethics is specifically addressed in several work programmes (WPs), for instance through **activity area 6.5 'ethics and justice'** in the 2007 WP. Here the programme aimed to address privacy, data protection and human rights issues, as well as acceptability, ethical issues and prioritisation questions[77].

'Ethics and justice' was first addressed as a dedicated activity area in the initial (2007) Security work programme, which called for proposals under two topics. Two projects resulted. The area was then omitted from the next (2009) work programme.

In 2010, the Review of Security Measures[78] for the LIBE committee noted that research on freedom and privacy constituted the weak part of the Security Research Programme, with only two projects funded under this area in the first (2007) work programme (accounting for 2% of all EC contributions at the time), and no relevant calls for proposals in the subsequent (2009) work programme.

[77] 'Work Programme 2007-2008 – Cooperation Theme 10: Security', European Commission C(2007)2460 of 11 June 2007).

[78] European Parliament (2010) Review of Security Measures in the Research Framework Programme. Study PE 432.740. Brussels.

The ethics and justice area then returned in the remaining Security work programmes (2010, 2011, 2012 and 2013), with a particular focus on privacy issues in relation to the development of technologies. Nine projects resulted from the 2011 and 2012 calls[79].

The eleven known projects funded in the ethics and justice area are listed in the table below. These represent around one-quarter of the projects, participations and EC contributions seen in the security and society cross-cutting mission area, and less than 5% of projects, participations and funding in the programme as a whole.

Table 42: Projects funded under area 10.6.5: Ethics and justice

Code	Acronym	Year	Participants	Cost	EC Contribution
218265	INEX	2008	9	€ 2,422,082	€ 1,890,248
217862	DETECTER	2008	8	€ 2,424,419	€ 1,869,684
261653	ADDPRIV	2011	10	€ 4,087,801	€ 2,818,338
261698	SAPIENT	2011	7	€ 1,631,967	€ 1,248,577
261727	SMART	2011	20	€ 4,191,658	€ 3,456,017
285166	COREPOL	2012	5	€ 1,775,192	€ 1,429,681
285492	SURPRISE	2012	12	€ 4,401,821	€ 3,424,109
285399	PRISMS	2012	8	€ 3,561,936	€ 2,985,745
285635	PACT	2012	13	€ 3,228,907	€ 2,675,108
285368	ALTERNATIVE	2012	8	€ 4,354,778	€ 3,423,262
313195	SECILE	2013	7	€ 811,001	€ 703,098
Total			**107**	**€ 32,891,562**	**€ 25,923,867**
Average			**9.7**	**€ 2,990,142**	**€ 2,356,715**

Source: Technopolis analysis of CORDA data, December 2014

The subsections below provide further detail on a selection of three of these projects (ADDPRIV, SURPRISE and SAPIENT), in order to better understand their contribution to ethical aspects of security research.

The example of ADDPRIV

Project title	Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance
Project Code	261653
Project type	CP - Collaborative project (generic)
Starting date	2011-02-01
Ending date	2014-03-31
Coordinator	Anova IT Consulting

The focus of the **ADDPRIV project** was to develop a new solution to limit the storage of unnecessary data whilst proposing technologies for automatic discrimination of relevant data recorded by a multi-camera network, based on the automatic identification of security-relevant events.

For the purposes of this case study, one of the most interesting aspects of the project was its aim to assist in the development of new ethical standards for surveillance systems that go beyond legal compliance. An Ethics Scoreboard and a Legal Scoreboard were developed as part of the project, which were based on an extensive analysis of the current legal frameworks and possible ethical issues that might be encountered. In order to strengthen the ethical and legal considerations, two external advisory boards were created, covering end-users and ethics respectively.

The example of SurPriSe

Project title	Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe
Project Code	285492
Project type	CP-FP
Starting date	2012-02-01
Ending date	2015-01-31
Coordinator	Oesterreichische Akademie Der Wissenschaften

79 Projects funded as a result of 2013 calls are not detailed within the project database extracted for the purposes of this study.

Security measures and technologies often involve collecting information on citizens, which raises questions about the level of violation of privacy. Citizens give up a certain amount of privacy in favour of increased levels of security, up to an acceptable point. However, there is no clear definition of this acceptable level of privacy violation.

The **SurPriSe project** aimed to investigate the relationship (trade-off) between citizens' security and personal privacy, and to answer fundamental questions, such as:

- What is an acceptable security technology in Europe, what is not and why?
- How do European citizens view the relationship between security and privacy?
- How do the views of citizens of different countries diverge on security and privacy?

The project involved about 2,000 citizens from nine European countries in participatory assessment activities. This resulted in confirmation of scepticism against the trade-off approach in general, with participants of the Citizen Summits and Citizen Meetings predominantly requesting strict limitations and regulations with regard to the use of surveillance technologies. These findings were also in line with conclusions and recommendations of other high level expert groups[80]. Since the project recently concluded (January 2015), there is no evidence yet of how the research will be applied.

The example of SaPiEnT

Project title	Supporting Fundamental rights, Privacy and Ethics in Surveillance Technologies
Project Code	261698
Project type	CP-FP
Starting date	2011-02-01
Ending date	2014-07-31
Coordinator	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung

The focus of the **SAPIENT project** was to develop and test a surveillance impact assessment (SIA) that could be used for evaluating the risks that surveillance systems, technologies, services or other initiatives pose for privacy, human rights and other ethical values. The project sought to help policy-makers, technology developers and others to better understand how and when smart surveillance should be used, and also to apply criteria to assure that such systems respect citizens' privacy and other values.

The project resulted in the first ever Surveillance Impact Assessment (SIA) methodology based on an evaluation of citizens' acceptance of surveillance technologies. In particular, the project identified the following three main principles to govern the development and deployment of surveillance systems:

- Surveillance systems should comply with the law;
- Surveillance should be used when there are not more cost-effective alternatives;
- Surveillance systems should be ethically defensible.

The SIA sets out a process to ensure that these principles are followed in order to safeguard ethical concerns. Again, due to the recent conclusion of the project, it is not yet known to what extent this methodology will be taken up.

In summary, these three projects – as well as the others funded in the field of ethics and justice – have contributed to advancing the knowledge around social acceptance and justifications around security technologies. This is highly pertinent in light of increasingly advanced technology and technology use that might deepen social mistrust towards security measures. Thus, the funding is dedicated to societal aspects of security research, helping to counterbalance and complement the strong industry focus of the other activity areas of the Programme.

[80] See for example European Group on Ethics in Science and New Technologies (2014), Ethics of Security and Surveillance Technologies – Opinion No. 28 or the Office of the United Nations High Commissioner for Human Rights (2014) The Right to Privacy in the Digital Age (A/HRC/27/37, 2014).

Individuals interviewed in the development of this case have, however, argued that the project results relating to social and ethical considerations of security research would benefit from wider dissemination, such that they could benefit developments in security technology and systems. Thus, future research actions in this area might benefit from placing greater emphasis on the intended impact of the ethical research.

F.1.5 Conclusions and lessons learnt

Ethics needs to be an integral part of security research actions to ensure that the project results are acceptable and socially justifiable. Including various horizontal and vertical mechanisms is an effective way to ensure this.

Ethical considerations at project level have sometimes gone beyond the checklist required by the European Commission. However, these approaches can be very costly and should therefore be limited to those projects that are of a highly sensitive nature as regards privacy, data protection and other pertinent human rights.

FP7 Security Research projects in the field of ethics have contributed to strengthening research on the societal aspects of security technology. This is a very important point in light of the extensive industry funding and technological focus of the Programme. However, the project results should be more widely disseminated to improve knowledge around ethics and security for the benefit of further research.

Ethics is an important consideration for security research, and poses very complex challenges. The FP7 Security Research Programme represented the first time that the EU has provided funding in the area of civil security research, but it has already made considerable progress in supporting greater consideration of ethical issues. It is important that ethics continues to be strongly represented, both horizontally and at the project level as part of future Security research programmes.

Several additional ideas have been suggested for the future, including:

- Strengthening the focus and guidance on conceptual ethics;
- Increasing funding to advance knowledge around ethics;
- Encouraging the follow-up by project officers of ethical considerations in projects, in order to ensure that end-results are socially justifiable and adhere not only to legal standards but also prevailing perceptions around security and privacy issues. This will help ensure that technologies and systems are not developed which later are rendered inapplicable;
- More widely disseminating the results of specific ‘ethics’ projects.

F.2 Forms of end-user involvement in projects

This case study explores the extent to which end-users have been involved in FP7 security research projects, how they have been involved, and what the benefits of this this involvement have been. In particular, it looks at a selection of cases where end-users have assumed the role of project coordinator, and examines the approach taken in these cases to maximising the involvement and input of end-users. The case contributes to the evaluation of the relevance of the Security Research programme to end-users and the beneficial effects of their involvement.

The case begins with an introduction, which gives an overview of the rationale for involving end-users and provides a definition of end-users of security research. The subsequent section analyses programme data from CORDA to determine the level and type of end-user involvement in the FP7 Security Research programme. The case then presents feedback from end-users about their involvement in the programme. The penultimate section then explores three end-user-coordinated projects in more detail. The case concludes by drawing conclusions and lessons learnt for Horizon 2020.

The cases study is based on analysis of a survey of end-users of the FP7 Security Research Actions and programme data from CORDA, complemented by four in-depth interviews with end-users representing three FP7 Security Research projects.

F.2.1 Introduction

The FP7 Security Research programme was conceived as an **end-user driven**, application-based research programme, and the importance of involving users directly in projects was stressed in annual work programmes and in guidance for applicants.

The Council Decision concerning FP7[81] defined the **objectives** for the Security theme as including stimulating the cooperation of providers and users for civil security solutions, and delivering mission-oriented research results to reduce security gaps. The subsequent Work Programmes for the Security programme also specified that cooperation between the end-user and supply side of security technologies and solutions should be a central feature of projects.

Furthermore, the direct involvement of end-users in the projects as participants was expected and encouraged, in order to guarantee the involvement of all the actors necessary for the development and demonstration of the systems. The testing, validation and demonstration of security solutions developed in projects, involving the end-users as much as possible, was also considered at the core of the Security theme.

End-users of security technologies, tools, products and systems therefore represented a **strategic stakeholder** in the FP7 Security Research Programme, and it was hoped that their inclusion and active participation in projects would help to ensure that final products would satisfy needs and could reach their relevant market more easily.

End-users are thought to have constituted a **significant minority** of the organisations participating directly in FP7 Security Research projects, and are known to have also been engaged with the programme through other routes such as project advisory boards and dissemination events. However, there is no formal monitoring and classification system that allows for the exact determination of end-user involvement.

As part of the wider evaluation of the FP7 Security programme, a **simple typology of end-users** was developed that could serve as a basis to identify and group end-users.[82] This defined end-users as private and public organisations that may apply or make use of security technologies, equipment or services developed in an FP7 funded project in providing their security service (of protection, support, aid, enforcement, emergency response, etc.). While such a definition excludes some organisations that are indirectly involved in security, this was necessary to have a clear analytical basis.

[81] Decision No 1982/2006/EC.

[82] The typology is contained in Appendix C.

In addition to "end-users in the strict sense" above, for the purpose of this evaluation, **policy-making bodies** were included. These could be legislators or rule-making bodies using the results of security research for drafting regulations, or agencies that develop strategies to address risks – but not organisations defining overarching policies at a higher level.

Based on these considerations the following 5 categories of end-users were defined:

- Emergency services;
- Public & private security services;
- Operators of / companies with critical infrastructure;
- Disaster relief and crisis management organisations;
- Policy-making bodies.

F.2.2 End-user involvement in the FP7 Security Research programme

Analysis of programme data (CORDA) provides some indicators of direct end-user **participation** in the FP7 Security Programme. Of the 3,741 participations in the Programme, 411 participations (11%) were from Public Bodies (excluding research and education) (PUB), while 3% were from 'other' types of organisations. Both categories are likely to be dominated by end-user organisations, as defined by the study.

As part of the survey of FP7 Security project participants also undertaken for the study, over 200 of those who responded (some 26%) identified their organisation as being an end-user of Security Research (based on the definition provided). If this rate were applied to the total number of organisations participating in the programme (1,824), then somewhere in the region of 470 participants are likely to have been end-users. Again, this demonstrates the significance of the group to the programme.

These end-user participants, as well as a small number of identified non-participating end-users were invited to participate in a further questionnaire survey specifically aimed at this stakeholder group. In total, 108 responses were received, and these replies provide further indications as to the involvement and experiences of end-users.

The end-user respondents came from 25 different countries, and represented a range of different types of end-user organisation, as follows:[83]

- Public and private security services (19%);
- Emergency services (18%);
- Operators of / companies with critical infrastructure (10%);
- Disaster relief and crisis management organisations (9%);
- Policy making organisations developing security regulations or strategies (9%);
- Other (34%) – commonly a security research and manufacturer, or operator / provider of technological tools or services.

Most (92%) of the respondents had **participated** in at least one FP7 security project, including 17% that had taken the role of **project coordinator** in at least one case. In addition, many had (also) been involved in the programme in other ways:

- 54% had **attended dissemination events** of an FP7 security project;
- 28% had **contributed expert advice** as part of programme definition or the contents of the work programme;
- 29% had been involved in the **expert advisory group** of an FP7 security project.

[83] The percentages shown do not sum to 100% due to rounding.

F.2.3 Feedback from end-users on their involvement in the programme

Despite widespread involvement in the programme amongst respondents, when asked about their level of **familiarity** with the FP7 Security Research Actions more generally, only half (54%) claimed that they were 'familiar' or 'very well informed' about it (the remainder reporting they were only 'somewhat' or 'not at all familiar').

End-users were also asked **how useful** involvement in the Security Research programme had been for their organisation. The response was very positive, with a majority (59%) claiming it had been 'very useful', and a further 35% claiming it had been 'somewhat useful'. When asked further about what the most important **benefit of involvement** had been, end-users commonly reported the following aspects:

- Increased opportunities for collaboration and networking;
- The development of new technological solutions;
- Improved knowledge, capabilities and understanding of security issues;
- Opportunities to affect security policy and future research efforts;
- An increase in the visibility of the organisation at EU level;
- Funding for Security R&D activity.

However, despite the perceived usefulness of involvement and the range of benefits cited, less than half (45%) of responding end-users felt that overall the benefits of involvement had outweighed the costs, while 28% felt costs outweighed benefits. A quarter (27%) felt the costs and benefits were broadly equal. While the net result is positive, one might hope that all (or at least a majority) of end-users would report a positive **cost-benefit assessment** of their involvement in the programme.

The issue was explored further, with end-users asked through the survey what the most significant barrier was to the realisation of benefits from the programme. The most commonly mentioned issues included:

- **Excessive administrative requirements** – including excessive reporting and financial administration and requirements, as well as the long time to grant;
- **Poor cooperation within the consortium** – caused by poor project coordination, cultural differences, the large size of consortia, and the different motives and priorities of participants;
- **A lack of resources** – both in terms of the time and money needed to produce the desirable results;
- **Insufficient use of end results** – resulting from a focus on academic outputs, the inaccessibility of results, and a lack of follow-up;
- **A lack of end-user involvement** – with a lack of end-user engaged in projects or being engaged too late, and end-user requirements not being sufficiently taken into account in project design.

Some of these issues / barriers, and particularly the last point on the involvement of end-users within projects were also picked up through the stakeholder interviews undertaken for the study.

Discussions with end-users suggested that the most common motivation for end-users to participate in FP7 projects is the expectation that, at the end of the project, they will obtain a final product that is ready to be deployed. However, at the same time, end-users have complained about the fact that they were involved only at later stages of project activities, when the testing of a prototype was required, and were not given an opportunity to contribute to the definition of product requirements. This created a gap between end-user expectations and the final output of the project. Ultimately, such gaps can have a negative impact on the effectiveness of the projects, their results and of the programme more generally. Project outputs cannot be deployed in the operational environment if they do not correspond to the real needs of users.

There is also a perception that project ideas are often driven by partners from research organisations and academia, who define project objectives, the intermediate steps needed to achieve the results and the structure of the project. Only then does a search take place for end-users to involve in the consortium and provide support for the testing phase. As a consequence, the testing activity is the only moment in which end-users can provide feedback to the technology developers and input specific requirements for the product. For end-users, it is not particularly useful to define and set requirements only in these final stages of the project, because there is then not enough time for the prototype to be modified accordingly. The output of a project is not a deployable solution as a result, but instead a prototype that can be used only after significant post-project modification.

Another issue that has emerged through the evaluation relates directly to the structure of FP7 itself and its procedures. In the security sector, end-users will often have very specific needs that require an immediate solution. FP7 research actions on the other hand have relatively long administrative procedures and implementation times. Thus there is a disconnect between the time horizons of security end-users and the procedures and duration of FP7 projects. There is also a general sense that end-users are at a rather early stage in their ability to articulate needs in terms of research due to their intrinsic concern with immediate operational issues.

F.2.4 FP7 Security Research projects coordinated by end-users

As introduced above, around one-in-five of the end-users responding to the end-user survey reported having coordinated an FP7 security project. The relevant organisation, and the project they coordinated are listed in the table below.

Table 43: FP7 Security projects coordinated by end-users

Acronym	Project Title	Coordinator
NMFRDISASTER	Identifying the Needs of Medical First Responder in Disasters	Magen David Adom, IL
DEMASST	Security of critical infrastructures related to mass transportation	Swedish Defence Research Agency (ROI), SE
PREVAIL	PRecursors of ExplosiVes: Additives to Inhibit their use including Liquids	Swedish Defence Research Agency (ROI), SE
SECURECHAIN	Integration of Security Technology Supply Chains and Identification of weaknesses and untapped potential	INOVAMAIS, PT
OPTI-ALERT	Opti-Alert: Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication	Fraunhofer, DE
SMART	Scalable Measures for Automated Recognition Technologies	University of Malta, MT
ADVISE	Advanced Video Surveillance archives search Engine for security applications	Engineering Ingegneria Informatica spa, IT
SCINTILLA	Scintillation Detectors And New Technologies For Nuclear Security	Alternative Energies and Atomic Energy Commission (CEA), FR
ICARUS	Integrated Components for Assisted Rescue and Unmanned Search operations	Royal Military Academy, BE
SUBCOP	Suicide Bomber Counteraction and Prevention	Swedish Defence Research Agency (ROI), SE
UNSETH	Unique Smart anti-tampering and Enveloping TecHnologies	Thales communications & security
HOMER	Homemade explosives and recipes characterisation-Capability	Police Service of Northern Ireland, UK
ATHENA	Athena	West Yorkshire Police, UK
RAIN	Risk Analysis of Infrastructure Networks in response to extreme weather	Trinity College Dublin, IE
EVIDENCE	European Informatics Data Exchange Framework for Courts and Evidence	National Research Council (CRN), IT

Source: CORDA database, based on self-identified end-user coordinators (end-user survey)

Below **three of these end-user-coordinated projects** are introduced and explored further, in particular their strategies and approaches to the involvement of end-users.

- Within these three projects, end-users were pro-active in trying to solve the problems highlighted above, by taking on the role of project coordinator and in their project design and approach. Those consulted believe that – as end-users - they were able to bring real added value to the consortium, as well as benefits to their own organisation.

- By taking the role of coordinator, they could influence the output of research and development activities, and make sure that the projects developed useable outputs for the operational environment. The role also offered end-users an opportunity to expand their network of technology suppliers and to consolidate and strengthen relationships with research organisations.
- All three projects demonstrate an **early involvement** of end-users in activities, already at proposal stage, in particular in the definition of the specific requirements regarding the final output, which are then translated in technical requirements by the research organisations participating in the action.

The example of ICARUS

Project title	Integrated Components for Assisted Rescue and Unmanned Search operations
Project Code	285417
Project type	CP-IP
Start date	2012-02-01
End date	2016-01-31
Coordinator	Belgian Royal Military Academy
Project website	http://www.fp7-icarus.eu/

The ICARUS project seeks to develop innovative **robotic solutions** that can provide unmanned search and rescue (SAR) technologies for detecting, locating and rescuing humans. The use of unmanned search and rescue devices - embedded in an appropriate information architecture and integrated into existing infrastructures – can provide detailed and easy to understand information to crisis personnel about a specific situation (e.g. real dangers present on the ground), and therefore improve crisis management capabilities in resolving a situation.

The project **rationale and objectives** are clear as to the focus on end-users and the engagement of end-users. The project promotional material highlights that there is an abundant literature on research efforts towards the development of unmanned Search and Rescue tools, but that this contrasts to the practical reality in the field, where unmanned search and rescue tools have great difficulty finding their way to the end-users. The ICARUS project therefore sets out to address this issue, by aiming to bridge the gap between the Research community and end-users.

In addition to being led by the Royal Military Academy of Belgium, two other main end-users are also part of the **consortium**: the Portuguese Maritime Rescue Command Centre (for Maritime Search and Rescue) and the Belgian First Aid and Support Team (for Urban Search and Rescue) – who serve as specific end-user contact points for the project. In addition, a majority of the other partners are companies involved in the development and sale of related technologies, in areas such as spacecraft, mapping, optomechanics, engineering, vehicles, wireless communications, lighting and machinery. Partners also include organisations specialised in transferring technology from academia to users.

One of the first activities of the project was the definition of end-user requirements. An **end-user board** – comprising experts in the field of search and rescue – was established to provide project partners with expert advice throughout the project. In addition, **interviews** were carried out with other key search and rescue stakeholders who could not commit to becoming board members.

The consortium deliberately adopted an approach focused on maximising the involvement of end-users, to make sure that technical requirements were defined as early as possible, paving the way for the technical development of appropriate solutions. Based on end-user requirements, the consortium has now started developing platforms and tools.

The ICARUS developments are intended to be **validated and demonstrated** this year, using two major demonstration events: a simulated earthquake exercise in Belgium and a maritime accident exercise in Portugal. The first is planned for September, and will involve multiple unmanned ground and aerial vehicles, equipped with powerful sensors, being deployed in a simulated crisis management exercise. A set of training and support tools developed by ICARUS will also be demonstrated, facilitating the use of these unmanned tools by end-users.

The example of HOMER

Project title	Homemade explosive and recipes characterisation
Project Code	312883
Project type	CP-FP
Start date	2013-11-01
End date	2016-10-31
Coordinator	Police Service of Northern Ireland
Project website	http://www.homer-project.eu/

The goal of the HOMER project is to expand the knowledge of European bodies about Home Made Explosives, in order to increase the security of the European citizens and support Europe's current and future security needs. Specifically, it aims to draft a fundamental standard for home made explosives and develop a **knowledge management platform**, which will improve the capacity of security and law enforcement agencies, as well as precursor manufacturers, to deal with homemade explosives threats. The project focused on the end-users' operational needs, in order to develop applicable products that can be implemented in the operational environment.

The approach to this project assigned a fundamental role to end-users from the start. In particular, they provide the research and technical partners with detailed information concerning their **operational needs**, ensuring that the products developed can be implemented in the operational environment. These requirements have been taken into account in the early stages of the research activity.

Conscious of potential communication and understanding issues between different types of partner, the coordinator has then put particular effort into **translating the operational requirements** (specified by end-users) for the research and industrial partners, who themselves do not have a background in operational security.

The example of EVIDENCE

Project title	European Informatics Data Exchange Framework for Courts and Evidence
Project Code	608185
Project type	CSA-SA
Start date	2014-03-01
End date	2016-08-31
Coordinator	Consiglio Nazionale delle Ricerche CNR
Project website	http://www.evidenceproject.eu/

The **use of electronic evidence** has become a necessary element to solving crime – both for the increasing number of crimes committed by use of electronic means and devices (cybercrime), but also for those that are not – and is therefore also acquiring increasing importance in lawsuits. However, there are a number of gaps, issues and inconveniences that are becoming evident as evidence increasingly migrates from paper documents towards a virtual environment, which require the development and widespread use of new technologies, as well as common understandings, processes and procedures associated with these.

The EVIDENCE project aims to provide a **road map** (guidelines, recommendations, and technical standards) for realising a Common European Framework for the systematic and uniform application of new technologies in the collection, use and exchange of evidence. This road map, incorporating standardised solutions, will enable policy makers to realise an efficient regulation, treatment and exchange of digital evidence. It will also allow Law Enforcement Agencies, as well as judges/magistrates, prosecutors and lawyers practising in the criminal field to have at their disposal a Common European Framework, allowing them to gather, use and exchange digital evidence according to common standards and rules.

The CNR institute involved as coordinator, the Institute of Legal Information Theory and Techniques, is a scientific and technological research institute focused on the impact of information and telecommunication technologies on law-related activities. However, it also falls under the study's end-user classification, as its activities include providing administrative support and training in the field of legal information, as well as the maintenance, update and distribution of legal and law-related databases.

Other end-users in the consortium include INTERPOL, the Council of Bars and Law Societies of Europe, the Law and Internet Foundation, and the Centre of Excellence in Information and

Communication Technologies. The responsibilities of the former two in the project are briefly presented here to illustrate **common ways of end-user involvement** in security research projects:

- INTERPOL will provide an overview and a status quo assessment of the collection, preservation and exchange of electronic evidence from the standpoint of law enforcement, and proposing guidelines that could be integrated into a Common European Framework governing this field.
- The Law and Internet Foundation will lead the dissemination and stakeholder awareness activities, ensuring dissemination of project information and results to, and relevant feedback from, a broad set of stakeholders.

In order to **validate the proposed technical specifications** and guidelines that will be developed through the project, and to test the developed proof of concept application, the project will also engage end-user organisations. EVIDENCE team members will organise specific events targeting audiences from end-user organisations, and also disseminate the results of the project through existing events of the legal and cyber crime/computer forensic community.

An external advisory group, consisting of experts and practitioners in the field of evidence collection, e.g. from the police, public prosecutors, the judiciary and civil rights groups, is responsible for overseeing certain aspects of the EVIDENCE project, including through providing external input, advice and feedback throughout the project, facilitating the involvement of affected stakeholders, and assisting the project partners in achieving impact.

The approach developed by the EVIDENCE project is therefore based on the inclusion of key end-users not only in the **validation phase**, but also and most importantly in the **identification of the shortcomings** of the national legislations (from which needs arise) and the **proposition of** guidelines and best practices to adopt.

F.2.5 Conclusions and lessons learnt

The main **motivation** for end-user participation in FP7 projects is the expectation that, at the end of the project, they will obtain a final product or tool ready to be deployed. However, there is often a gap between the initial expectations and the final outputs of the projects, caused by the fact that their concept, definition and management is often driven by research and industrial organisations. The consequence is the development of outputs that don't always correspond to end-users' needs and requirements, and so cannot be immediately deployed in operational environments.

Projects coordinated by end-users appear to adopt a proactive approach towards the inclusion of end-users, focused on the role they have to play in defining the specific requirements of the new technology, ensuring that the research and development performing partners deliver tangible outputs that are immediately usable. The approaches adopted in the projects in which end-users have taken the role of coordinator show significant differences, aimed at overcoming the identified issues and deliver fit for purpose outputs. The presented projects are not yet finalised, but it is possible to draw some conclusions regarding the benefits of end-user led projects.

In particular, these projects tend to include the following **features**:

- End-users are involved in the initial phases of a project[84], with the objective of defining the operational requirements of the tool or product that will be developed. These requirements are then translated into technical specifications by the research and industrial partners;
- End-users are in charge of specific work packages in which the aim is to define specifications and requirements, but also to propose solutions;
- Projects increase the amount of information obtained from end-users and use it during the research and development phase, instead of assigning to end-users only the role of final

[84] In general, if projects are coordinated by end-users, end-users have already been involved at the proposal stage.

testers. Other than direct participation in consortia, end-user input and involvement is also ensured through external advisory boards contributing expert opinions, and consultations on specific issues, e.g. through interviews;

- Project objectives reflect the need to develop and deliver a product or tool that is fit for purpose from the point of view of end-users, rather than the research performing partners, and is ready to be deployed in the operational environment;
- Communication and dissemination activities are clearly targeted towards end-users.

According to end-users participating in FP7 Security Research projects the only way for projects to deliver outputs that are fit for purpose, immediately deployable at operational level, and that can contribute to solving real-life needs, is to actively involve them **throughout the entire process** of the preparation, management and review/evaluation of the Security Research programme. While a number of measures have been put into place, the Commission could explore further ways to strengthen end-user involvement in the future. For example:

- At the proposal stage, more end-users should be involved in the proposal evaluation process.
- In order to ensure that the programme achieves its strategic objectives of improving the security of European citizens and of increasing the competitiveness of the security market, H2020 work programmes should better take into account the strategic role of end-users and design targeted mechanisms to maximise their input in the projects. For example, the Commission could make it a mandatory requirement to involve end-users as direct project participants – rather than just in advisory bodies – in any project that aims to produce outputs above a certain TRL. Similarly, all projects should be required to set aside from the beginning a part of their budget for specific activities targeting end-users.
- End-users can play a crucial role in testing and validating research results and in the valorisation of research outputs. The Commission should explore how end-users could play more active roles in the dissemination of project results and how they could be motivated to take up the results of other security research projects, e.g. by attending dissemination activities of other projects or by being actively involved in Communities of Users.
- The uptake of research results can be further supported through the application of new instruments provided by H2020, in particular of Pre-Commercial Procurement (PCP) and Public Procurement of Innovation actions (PPI) to steer the development of solutions towards concrete public sector needs whilst comparing/validating alternative solution approaches. End-users are key actors for the successful application of these instruments, as they enable field testing and intense feedback. The Commission should provide end-users with specific information about the opportunities that the new instruments offer for them.
- These instruments might also be useful to address another problem that many end-users face: meeting short-term innovation needs rather than mid- to long-term research needs. End-users often have quite specific requirements that ask for an immediate solution, while the projects under the FP7 Security Research Programme have much longer timeframes. Therefore, the Commission should – across the different DGs – explore ways to provide quick funding for innovation addressing the short-term needs of end-users.

F.3 Shaping the end-user landscape in the EU

This case study examines how the FP7 Security Research Actions stimulated the cooperation of providers and users of civil security solutions. The objective is to analyse the different ways in which end-user communities have been structured in different sectors, in order to identify good practices and any other lessons that might be learnt from these experiences. Three specific end-user communities are considered:

- In the Customs sector, the European Customs Detection Technology Expert Group;
- In the CBRN-E sector, the Community of Users (CoU) on Disaster Risk and Crisis Management;
- In relation to law enforcement, the European Network of Law Enforcement Technology Services (ENLETS).

The case contributes to the evaluation of the **involvement of end-users** and barriers to the effective implementation of the FP7 Security Research Actions. Below, a general introduction to issues surrounding end-user involvement and coordination is given before each of the three examples of end-user communities are analysed. The final section presents conclusions from the case and draws lessons for Horizon 2020.

The research conducted in the development of the case study included desk research and interviews with three experts (from the Commission and end-user networks).

F.3.1 Introduction

The FP7 Security Research programme was conceived as a user-driven, application-based research programme that would provide support to **end-users** of security related technologies and strengthen their capacity to respond to threats to citizens' security. Indeed, the Decision concerning FP7[85] defined the objectives of the Security Research theme as including stimulating the cooperation of providers and users for civil security solutions, and delivering mission-oriented research results to reduce security gaps.

The subsequent Work Programmes also specified that **cooperation between the user and supply side** of security technologies and solutions should be a central feature of individual projects. End-user involvement was seen as a way to achieve a better-targeted programme and projects, as well as to develop and deliver innovative solutions that could be immediately deployed in response to security threats.

However, several **issues** have emerged during the wider evaluation of the FP7 Security Research Actions. It suggests there is further need for better coordination and involvement of end-users in the design, delivery and exploitation of Security research:

- The involvement of end-users only in the final stages of many FP7 security research projects, specifically during the testing phases, is thought to have caused delays in the development of final products. Instead of being a phase of validation for a specific technology, testing can be the only moment where end-users are given the opportunity to assess the potential of a prototype and to communicate their technical requirements to the research and development partners;
- Projects funded under the FP7 Security Research theme are felt to have often lacked adequate communication strategies to reach relevant end-users and policy makers, causing difficulties for, and limiting the degree of, uptake of final project results;
- The parallel implementation of a large number of related projects creates knowledge and other results that are not particularly well-coordinated, aggregated or filtered, either between the different projects themselves, or to end-users. There is no common platform in place to exchange information, boost awareness and transfer relevant research projects to relevant users.

[85] Decision No 1982/2006/EC.

Nevertheless, one of the major benefits of the FP7 Security Research Actions cited by stakeholders is the **impact** that the programme has already had on the end-user scene in Europe. Not only did end-users become involved as project participants, they also started to organise themselves in reaction to the research programme.

Partly in an effort to address the issues identified above, communities have begun to be established that provide end-users, research organisations, industries and policy makers, with a **forum** in which to share information, technical specifications, needs and ideas, so as to achieve more effective project results, better programming and faster uptake of developed technology.

F.3.2 The end-user community in the customs sector

EU **customs policy** seeks to facilitate legitimate trade, whilst applying the level of controls necessary to guarantee the safety and security of citizens, and to protect the health, environment, financial and economic interests of the EU and its Member States. This policy, and increasing threats from e.g. terrorism have expanded customs to become a major player in the field of supply chain security.

The deployment of modern **technologies** plays an essential role in enabling customs administrations to meet these strategic challenges, and there has been an increasing need amongst national customs administrations for access to better tools, technologies and systems to enable them to implement more effective responses to evolving threats.

As such, the involvement of the customs community (i.e. the end-users) in research and development is important if these intended beneficiaries are to gain access to, and extract benefit from, relevant and appropriate technologies and solutions.

In 2011 the Directorate-General for Taxation and Customs Union (DG TAXUD), together with national customs administrations, created a **European Customs Detection Technology Expert Group (CDTEG)** consisting of customs detection technology experts from twelve Member States[86].

The group was intended to serve as a platform for **sharing information** between customs technology experts, and as a forum in which end-users of security technologies could **define the needs** for new and improved technologies. This would include analysing current threats; making forecasts as to the evolution of these threats in the short-, medium-, and long-term; and assessing the technologies, tools and systems needed to successfully overcome these threats[87].

The group produced several **outputs** during its initial mandate period (2011-13):

- It compiled a list of available detection equipment in EU Member States;
- It linked detection equipment to border type, transport mode and risk category;
- It delivered short-, mid- and long-term recommendations to shape the future use of detection technology;
- It provided guidance on the construction of detection architectures.

The documents and guidance materials produced by the CDTEG gave an overview of existing detection capacity and capability, as well as current and future threats. They therefore provided a solid basis for discussions between EU customs administrations and the EU security industry, research institutes and academia, as to future R&D activities and their alignment with end-user (customs) requirements and needs.

Indeed, inputs from the CDTEG process were formally communicated to the **FP7 Security Research** programme, such that they might be taken into consideration in subsequent work programmes and calls for proposals. According to those interviewed for this case, this process has been of strategic importance for customs end-users. As such, the CDTEG provided the only formal source of detailed information to ensure that FP7 Security Research programme topics

[86] Austria, Denmark, France, Hungary, Ireland, Italy, Lithuania, the Netherlands, Slovakia, Spain, the UK and Turkey.

[87] van Heeswijk, W. (2015) Towards Rationale Use of Detection Technologies, DG TAXUD (presentation).

corresponded to the real needs of users in the customs sector. The interviewees believe that the process has translated into better defined work programmes and topics in the calls for proposals, which are closer to the real needs of end-users and which address specific issues identified by them. The MODES, AXCIS and HANDHOLD projects were given as examples of research actions that address needs discussed by the community of users.

A **workshop on Customs detection technologies**, organised under the Customs 2020 Programme of the European Commission and held in October 2014, is a further interesting development – building on the work of the CDTEG. The event was organised to share knowledge and build synergies between the research community and end-users, to identify needs, to draft common specifications, to share testing equipment and to support control operations with the use of modern detection technologies. It sought to analyse current capabilities and the limitations of available technologies for custom control, which would then lead to the identification of specific areas where improvements could be made.

The participation of research organisations, universities, technology providers and end-users in the workshop allowed for direct discussions about future synergies to bridge the gap between end-users' needs and technology solutions. The workshop also resulted in a set of **recommendations**, which included:[88]

- Improving and strengthening the joint activities between customs administrations and industry, in order to define specific requirements, provide guidance to the research and industry communities to ensure a development of new technologies coherent with the needs of end-users;
- Increasing information sharing among countries, for example through common libraries of data, common list of existing equipment and best practices;
- Developing the use of common platforms for contacts between authorities and industry and for high-level contacts between worldwide Customs authorities.

Building on the success of this first event, a second customs detection technologies workshop is due to be held in 2017.

F.3.3 Community of Users on Disaster Risk and Crisis Management

A Community of Users (CoU) has also recently been established in the area of disaster risk and crisis management. It includes actors addressing risks arising from Chemical, Biological, Radiological, Nuclear agents and Explosives (CBRNE), as well as natural and man-made disaster risk reduction (linked to civil protection) and disaster management. The community **aims** at sharing information among all the key players in the fields and at ensuring a proper transfer to and application of research outputs by users. The community is part of a wider effort to strengthen cooperation in the disaster risk and crisis management sectors.

Several key EU policies set the general **framework** for security strategies regarding disaster risk and crisis management and the research in this area such as the EU Agenda on Security[89] establishing a security policy framework, the Security Industrial Policy[90] aiming to boost industry competitiveness and innovation or the EU research policy[91]. The specific framework for the activities in the area of disaster risk and crisis management is set by a number of programmes and instruments, for instance:

- **CBRN-E** threats are addressed by a range of international, European and national policies. The key EU policies are the EU Action Plan on Enhancing the Security of Explosives[92] and

[88] EC, Hungarian National Tax and Customs Administration (2014), 1st workshop on customs detection technologies, Overview and report (presentation).

[89] COM(2015) 185 final.

[90] COM(2012) 417 final.

[91] Decision No 1982/2006/EC.

[92] Doc. 8109/08 and Regulation 98/2013.

the CBRN Action Plan[93] (DG HOME). CBRN is also included as a focal point in other policies, e.g. related to civil protection, consumer health protection, energy infrastructure and transport networks, customs, and environment and industrial risks;

- **Crisis management** policies are addressed through the EU Civil Protection Mechanism, and operationally coordinated by the Emergency Response Coordination Centre (ERCC). Other policies and bodies are involved in disaster risk management such as DG HOME through the EU Agenda on Security, DG SANTE, or DG ENV and DG CLIMA tackling climate-related disasters. Finally, intergovernmental agencies such as the European External Action Service (EEAS) implementing the EU Common Foreign and Security Policy, or the EU Law Enforcement Agency Europol, assist EU Member States in this area.

The EU pursues an integrated approach that addresses the entire risk management cycle. It comprises preparedness/prevention, detection/surveillance, and response/ recovery for the management of natural and man-made hazards.

The implementation of these policies represents a **complex and ambitious challenge**, as each Member State tends to follow specific national approaches to dealing with disasters and crises and has different operational capabilities.

Moreover, both areas are scattered into many **different disciplines and sectors** and the different hazard-related communities are often working independently on overlapping crisis situations (e.g. experts dealing with climate extreme events vs. earthquake specialists). This makes cooperation across Europe and often even within one country challenging.

Finally, the **organisational set up of crisis management actors** varies considerably. For example, there are policy-makers and the general public, research organisations, industrial companies, and operational services such as first responders or training centres. The operational services are of a particularly diverse character: there are local (e.g. fire-fighters and, in some countries, the police forces), national (the police force in other countries) and international organisations (e.g. the Red Cross), private and public actors, as well as professional forces (as in Sweden) and organisations made up largely of volunteers (such as THW in Germany). As a consequence interests, cultures and organisational dynamics differ widely. This is one reason that several experts interviewed for the purpose of the evaluation pointed to when explaining why there is no EU-wide interest representation of operational organisations in the area of risk and crisis management and CBRNE.

The development of the **Community of Users responds** to the challenges outlined above by providing a common platform for sharing information and by bringing together key scientific, policy and industry actors, as well as end-users, around a common vision and strategy. It seeks to address these issues by enabling information sharing, common approaches and understanding, and the identification of needs.

The **Community of Users** on Disaster Risk and Crisis Management was established by DG HOME, with a first formal meeting held in November 2014, and plans to meet at least twice each year thereafter. It is composed of interested DGs, representatives from the EDA, Europol, national ministries, industry, SMEs, research organisations, technical consultants and end-users. The community is intended as a means to share information between different stakeholders on research and policy developments, to promote greater alignment and complementarity in approaches to research and policy, and ultimately to stimulate common demands.[94]

One activity undertaken in preparation for the creation of the Community was the development of **research and policy mapping**. The developed matrices mapped all the policies addressing disaster risk and crisis management including CBRNE, natural and man-made disasters, as well as the technological developments and future trends, and provided information regarding the relevant FP7 projects. This on-going exercise is designed to enhance policy coordination both at

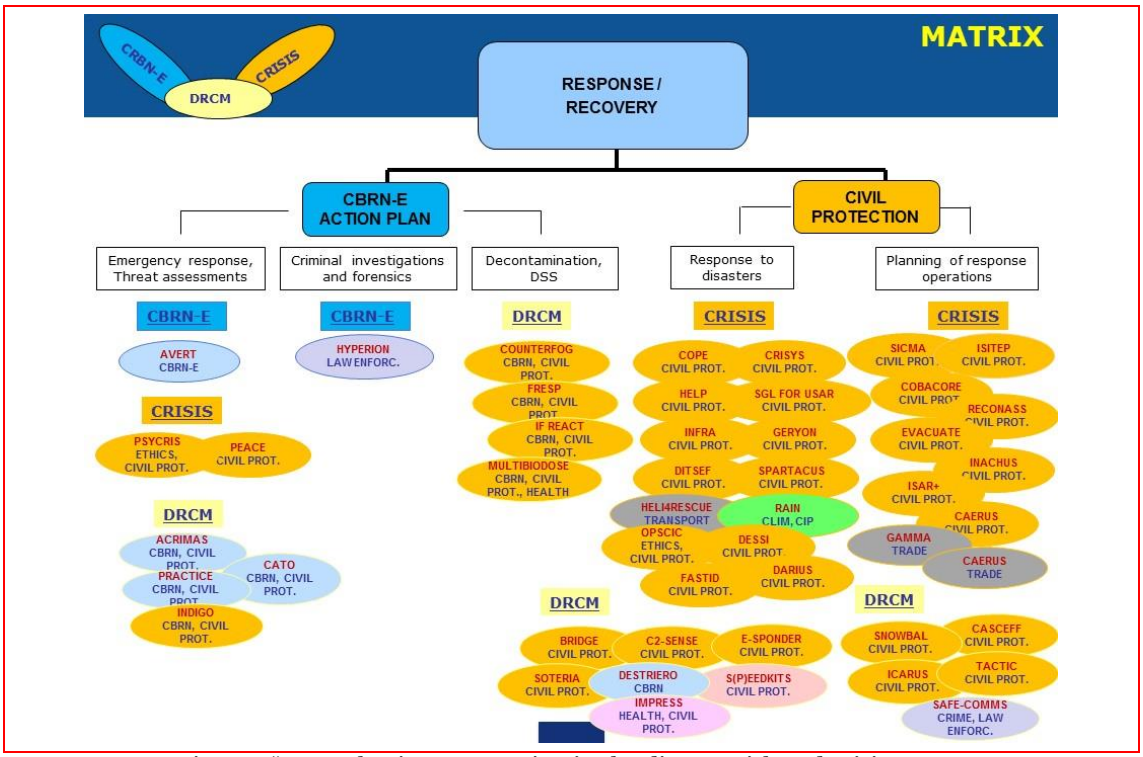
[93] COM(2009) 273 final and COM(2014) 247 final.

[94] A Community of Users on Disaster Risk and Crisis Management – Building on a mapping of EU policies and their links to technical and scientific challenges, EUR Report, DG HOME, in preparation.

programme and operational level, in order to avoid duplication of efforts and ensure that synergies among policy, research, industry and operational services are created.

For end-users, an important output of the process is a **mapping of FP7 Security Research projects** and their interaction with other policies. This is a fundamental feature, allowing end-users to obtain detailed information on project results and the potential for the use of such solutions for their operational activities. The figure below shows an example of such a matrix connecting key policies and projects.

Figure 27: Example for mapping of FP7 Security Research projects



Source: Presentation on "Strengthening cooperation in the disaster risk and crisis management sectors – Perspectives within Horizon 2020"; Example: response/recovery. DG HOME, 2015.

F.3.4 European Network of Law Enforcement Technology Services (ENLETS)

The European Network of Law Enforcement Technology Services (**ENLETS**) was set up in 2008 on the initiative of the Police Cooperation Working Party[95], as a platform to share information and network between national law enforcement agencies (end-users responsible for implementing new technologies in police departments within Member States) and those parts of industry, research and academia with an interest in the development of law enforcement technologies.

It is an **informal network** with 26 participating countries (all EU MS, with the exception of Malta and Croatia). An ENLETS contact person in each EU country tracks technology developments and their potential applications for daily police tasks. This helps avoid duplication of different systems in EU Member Countries while supporting research goals that lead to cheaper and more interoperable capabilities. There is a Core Group of countries (Belgium, Cyprus, Finland, France, Greece, the Netherlands, Poland and the UK) that is tasked with representing the network and providing it with strategic direction. Two formal meetings are held each year for the purposes of road-mapping operational and technology trends, and for sharing end-user scenarios.

[95] One of more than 150 highly specialised working parties and committees that serve as preparatory bodies for the European Council.

The mission of ENLETS is to support "*front line policing and the fight against serious and organised crime by gathering user requirements, scanning and raising awareness of new technology and best practices, benchmarking and giving advice*"[96]. This reflects the tasks originally set out for the Network by the Council, which were that it should serve as a **central contact point** for Member States, law enforcement agencies, research and industry, and the Commission and should organise a **technology watch** function for internal security research and industrial policy tasks in Europe.

The Council, in 2013, also stressed that ENLETS should **enhance coordination** between Member States, and should (in the long-term) seek to become a leading platform for strengthening the involvement of internal security authorities in security-related research and industrial policy[97]. As part of this, it would ensure effective end-user involvement in both EU security research activities and industrial policy.

Specifically, the Council Conclusions gave a mandate to the ENLETS network to undertake the following **tasks**:[98]

- To monitor and coordinate the development of new technologies and support a proactive involvement with research institutes and industry;
- To develop an EU overview of the internal security authorities' user needs for relevant European Institutions, research institutes and the industry;
- To share best practices, innovative ideas and research projects in the Member States and Agencies;
- To assist in defining technical standards as references for Member States;
- To assist Member States in the design of public procurement of technology for law enforcement purposes;
- To provide technical advice to the European Commission on relevant procurement procedures;
- To explore funding opportunities (such as the Internal Security Fund and H2020), ensuring that law enforcement organisations participate in cooperation projects and activities with the relevant research organisations and industrial community.

As such, it is intended that ENLETS will play a fundamental role in coordinating and supporting the actions of law enforcement forces at EU level with regard to research and innovation, and in closing the gap between technology providers, the research community and end-users. Reportedly, the network has already supported a changed approach towards innovation and technology within Europe's police forces, which can be seen for example in the inclusion of innovation and technology assessment within police policies.

F.3.5 Conclusions and lessons learnt

A very important outcome of the FP7 Security Research Programme has been that end-users have not only started to actively participate in research projects, but they have also started to organise and network, creating end-user communities in various sectors. With the support of various DGs of the European Commission, end-users have organised into **sectorial communities** in areas such as disaster risk and crisis management including natural and man-made disasters, as well as CBRNE, customs, and law enforcement technologies, all of which have been considered in this case.

This process of shaping end-user communities began – at least in part – in response to the need to connect the definition of policy and programme objectives within the European Institutions

[96] Padding, P. (2013) ENLETS PCP Briefing, 15 November 2013 (presentation).

[97] Council Conclusions on strengthening the internal security authorities' involvement in security-related research and industrial policy, DOC 12103/13.

[98] Council Conclusions on strengthening the internal security authorities' involvement in security-related research and industrial policy, DOC 12103/13.

with research projects funded under the FP7 Security Research theme and, most importantly, with the needs and technical requirements of end-users.

The fundamental aim of these communities is to assess future threats, and the technologies needed to overcome these. They have three main objectives:

- Sharing information regarding policy developments and threats to security, and mapping the technological gaps that need to be bridged in order to ensure the protection of European citizens;
- Identifying and addressing the need for research, technology and policy, to enable a better design of funding programmes and opportunities at EU level;
- Transferring knowledge to policy makers.

The analysis of the experience in the customs, disaster risk and crisis management, and law enforcement sectors shows that, despite the differences between these sectors, common features emerge. In particular, the need for a better flow of information between policy makers, research and industrial communities and end-users leads to the creation of sectorial platforms in which the relevant stakeholders can contribute to the definition of research, project, and up to a certain extent, programme priorities. These coordination activities allow the creation of detailed maps of policy developments, technology evolution, current and future threats and end-user's needs, contributing to a better policy and programme definition, more effective project results and improved response capability for end-users.

These end-user communities have become key players in the EU security policy framework, with policy making and programme implementation processes now relying on the ability of end-users to effectively coordinate and communicate not only with the EU Institutions, but also with the research community and industry.

Lessons learnt for H2020

End-user communities are a reaction (in part) to a very specific problem that end-users were facing in the Security Research Programme: the gap between expected outputs and actual results. End-user communities sought to reduce this gap, by providing bespoke platforms and fora with the opportunity to share information, ideas, requirements and technical needs with the research and policy communities.

The already important role that the user communities play in the EU policy making and programming process **should be strengthened** under H2020. The formalisation by the European Commission of the role that end-user communities play in the formulation of policy and programme objectives would strengthen the capacity of these networks to provide first hand technical information, feedback and updates, and therefore contribute to the achievement of the overall objectives of the programme. Projects designed with a strong contribution of end-users allow for a faster definition of technical requirements and a faster testing phase, thus increasing the possibilities for the project to develop fully market ready technologies.

Interlocutors have also highlighted the **need to introduce simplified and faster administrative procedures**. The time frames of FP7 projects - around one year between submission and kick-off of the project activities – are considered excessively long and pose a serious constraint on the effectiveness of activities funded by the European Commission. A proposed solution would be the introduction of a "fast track to project" with faster procedures and access to funding, making it possible for end-users to design and deliver short term responses to sudden threats to the security of European citizens in cooperation with the research and industrial community.

F.4 Analysis of the complementarity of CBRNE security research in FP7 and projects involving EDA

This case examines the complementarity of research projects funded by the FP7 Security Research Actions, on the one hand, and projects overseen by the European Defence Agency (EDA), on the other, about chemical, biological, radiological, nuclear and explosive (CBRNE) hazards. In as much as the EDA oversees projects funded and pursued by its members, the case explores how effective FP7 Security Research is in engaging with and leveraging research activities on CBRNE in the Member States.

Following some introductory remarks about the broader policy background for the CBRNE research cooperation between the European Commission and the EDA, the case discusses this research coordination in greater detail. In particular it explains the need for coordination, before outlining how coordination activities have been implemented. The case then reflects on a number of issues and limitations of the coordination, before drawing conclusions and highlighting lessons learned for Horizon 2020. The case contributes to the evaluation of the **coherence of the programme** with the research activities of Member States.

The research conducted in the development of the case included document analysis, semi-structured interviews with four experts (from the Commission, the EDA and two companies involved in relevant research projects) and the analysis of statistical data collected in the CORDA database of the European Commission.

F.4.1 Introduction

The coordination of research activities between the European Commission and the EDA has evolved against the background of a wider policy to protect the EU from the hazards that might arise from CBRNE.

A number of **international agreements** guide EU and Member State policies on CBRNE. These have established international regimes to limit, monitor and (partly) control the use and spread of chemical, nuclear, radiological and biological agents. Chief among these conventions are:

- The Chemical Weapon Convention (CWC), whose implementation is controlled by the Organization for the Prohibition of Chemical Weapons (OPCW);
- The Nuclear Non-proliferation Treaty (NPT), controlled by the International Atomic Energy Agency (IAEA);
- The UN Biological and Toxin Weapon Convention (BTWC) (no control mechanisms)

At **EU level**, CBRNE hazards are addressed by a variety of policies. The key EU policies are the EU Action Plan on Enhancing the Security of Explosives[99] and the CBRN Action Plan[100]. CBRNE is also included as a focal point in other policies[101]. They provide the political framework for the research undertaken in this area and financed by the EC.

The main goal of the **CBRN Action Plan** is to prevent unauthorised access to CBRN materials within the EU.[102] This involves measures of prevention, and particular attention is paid to CBRN emergency planning, strengthening countermeasure capacity, reinforcing information flows, developing better modelling tools and improving criminal investigation capacity. The plan focuses on the required capability to detect CBRN materials in order to prevent or respond to CBRN incidents. This is related to the development of minimum detection standards to be applied across the entire EU, establishing trialling, testing and certification schemes for CBRN detection and improving the exchange of good practices on the detection of CBRN materials.

[99] Doc. 8109/08 and Regulation 98/2013.

[100] COM(2009) 273 final and COM(2014) 247 final.

[101] For details, see case study 3 in Appendix F.

[102] The EU Action Plan on Enhancing the Security of Explosives contains similar measures with regard to hazards stemming from explosives.

Most of these measures require extensive research, which is in part carried out through the FP7 Security Research Actions (discussed in greater detail further below).

The **European Defence Agency** (EDA) was established under a Joint Action of the Council of Ministers in 2004[103]. The EDA is an intergovernmental agency with participation from all-but-one Member State of the EU. Its mission is to support the participating Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the Common Security and Defence Policy (CSDP) that is part of the Common Foreign and Security Policy (CFSP). This includes the development of defence capabilities, creating a competitive European Defence Equipment Market (EDEM), strengthening the European Defence Technological and Industrial Base (EDTIB), and promoting defence research and technology.

The CBRNE field has been part of the action priorities of the EDA since its establishment, and the publication of the **Capability Development Plan** (CDP) in 2008. The CDP is a 'living document' that is regularly adapted, and it defines future short and longer term needs. It is the basis for generating and stimulating cooperative capability projects (new programmes or off-the-shelf acquisition), and for orientating research and technology defence investment. The Plan constitutes a key instrument for informing Member States' capability development in the CSDP context, identifying defence requirements from short- to long-term. Within the CDP, the protection against CBRNE threats is deemed a priority for investment in research and innovation.

Recent activity by the EDA in the CBRN area includes the development of minimum standards of proficiency for education and training for CBRNE specialists within the context of EU military operations and the organisation of exercises and workshops with national defence forces to support training to respond to CBRNE threats.

Against this policy background the EC and the participating Member States of the EDA developed research activities in the area of CBRNE.

F.4.2 Research coordination between the EC and the EDA

Dual use research and the need for coordination

Given that the FP7 Security Research programme has a strictly civilian character and the EDA focuses on cooperation in the military area, this case also addresses the question of dual-use.

Dual-use items are **defined** as goods, software and technology normally used for civilian purposes but which may have military applications. A considerable number of technologies and products are generic and can address the needs of both civil and military end-users, especially at lower technology readiness levels. CBRNE hazards represent one area that is tackled by both military and civilian operators, and both sectors are developing products and solutions to counteract such threats.

The 2004 **Group of Personalities** report[104] already pointed out that technology is often multi-purpose, with civil and defence applications increasingly drawing from the same technological base and hence, a growing cross-fertilization between the areas.

The 2006 Council Decision concerning FP7 clearly states that "*security research at Community level will maintain an **exclusively civil orientation** and focus on activities of clear added value to the national level. As a consequence, civil security research within the Seventh Framework Programme will reinforce the competitiveness of the European security industry. **Recognising that there are areas of 'dual-use' technology, close coordination with the** activities of European Defence Agency will be needed in order to ensure complementarity*".

The 2004 Council Joint Action establishing the **EDA**[105], tasked the Agency "*to work in liaison with the European Commission to maximise the complementarity and synergy between*

[103] 2004/551/CFSP of 12 July 2004.

[104] Group of Personalities in the field of Security Research (2004) Research for a Secure Europe.

[105] 2004/551/CFSP of 12 July 2004.

defence and civil or security related research programmes". Article 45 of the EU Treaty[106] sets out, among other things, that the EDA is to "*support defence technology research, and co-ordinate and plan joint research activities*". The article provides the basis for closer and innovative co-operation between military and civil research and development.

EDA began coordinating priorities for investment with the European Commission soon after its operational launch in 2005. In line with the approach, the **European Framework Cooperation for Security and Defence (EFC)** was established in 2011, when both institutions agreed to harmonise their research activities. The EFC was later joined by the European Space Agency.

The EFC seeks a "***systematic synchronisation*** *between R&T investment under the EDA umbrella and by the Commission – thus maximising complementarity of civilian security, space and defence-related research programmes*"[107]. The overall aim is to prevent duplication between defence and civilian research to save resources, and to improve civil-military interoperability and standardisation.

More specifically, the EFC aims to:

- Provide a platform for the exchange of information, ideas, priorities, experts and research results;
- Coordinate the implementation of their respective priorities and actions and avoid duplication of efforts;
- Create synergies between the two strands of research (civil and military);
- Build capabilities that meet the needs of defence and civilian security communities.

CBRNE research activities of the EC and the EDA

The research projects conducted by EDA for CBRN protection are coordinated with DG HOME under the EFC. Under the EFC, CBRNE was identified as a pilot case, in which to explore dual-use synergies especially in the fields of detection, protection and decontamination.

In total, **73 projects** have been conducted at EU level in the area of CBRNE. These projects have either been funded by FP7 Security Research Programme or through the European Defence Agency and its Joint Investment Programme for CBRNE (JIP CBRNE - see below).

Within the **FP7 Security Research Actions**, CBRNE research was not a specific mission area, but featured prominently in particular under the 'security of the citizens' (for CBRN protection and explosives) and the 'restoring security and safety in case of crisis' (for CBRN response) mission areas, as well in the fields of CBRN Protection, CBRN Crime, and CBRN Response[108]. In total, 62 projects in the CBRNE domain were funded through the programme involving various types of civilian end-users, including fire-fighters, emergency responders, police forces, hospitals, civil protection forces, customs administrations, and local and regional authorities. These projects have sought to provide, test and validate new solutions, tools, systems, equipment, protocols and standards in the area of CBRNE.

The EDA oversaw 11 projects through a Joint Investment Programme for CBRNE (JIP CBRN). This **JIP CBRNE** was launched in 2012 as a four-year, €12m programme, supported by 13 participating Member States. The JIP aims to examine and evaluate the next generation of technologies for countering CBRNE threats in both military and civil environments[109], and to address research, development and demonstration activities, ranging from system of systems down to the underpinning technologies. Through the JIP CBRNE, two calls for proposals were

[106] Consolidated version of the Treaty on European Union/Title V: General Provisions on the Union's External Action Service and Specific Provisions on the Common Foreign and Security Policy.

[107] European Framework Cooperation on Security and Defence, EDA Factsheet.

[108] More information can be found in European Commission (2014) EU Research for a Secure Society – Security Research Projects under the 7th Framework Programme for Research.

[109] EDA (2012) Annual Report.

issued in 2012 and 2014, and **11 projects** were selected for funding[110]. Most of these projects have a timeframe of three years, and so the final results will be available at the end of 2015. No further calls for proposals are planned.

Organisational implementation

Three years into this pilot, the cooperation between the Commission and the EDA on CBRNE research has developed mainly at **three levels**: in the management of programmes, the evaluation of project proposals, and the implementation of projects. Each is explored further below.

Regarding **programme management** the European Commission has taken part in the meetings of the EDA JIP CBRNE Management Committee and the EDA has participated in the meetings of the FP7 SEC Programme Committee since 2011.

They **regularly exchange information** on on-going and future activities, e.g. programme priorities, strategic objectives and activities, any problems and needs identified in the CNRNE field, and the results achieved from research with a particular focus on dual-use research domains. Cross-participation at the programme level has enabled a communication channel between military organisations and civilian entities, allowing for the coordination of strategies and solutions to common threats.

Starting with the 2011 FP7 Security call and the first JIP CBRN call the same year, experts from the European Commission and the EDA began participating as evaluators in the respective project **proposal evaluation processes**. This has continued for the 2012 and 2013 FP7 calls, and for the second JIP CBRN call. Personnel participated not as official representatives of their relevant organisations and associated initiatives, but rather as technical experts in the Security and CBRNE domains. This is an important distinction, which allowed the cooperation to take place within the EC rules. The process has provided an opportunity for input and insight into the activities of the respective initiatives.

As regards the **implementation of projects**, EDA representatives are participating in the advisory boards of three FP7 **projects** (EDEN, IFREACT and MIRACLE[111]), and have also been involved in the workshops, conferences, panels and demonstrations of another four (TWOBIAS, CATO, SLAM and EQUATOX)[112]. Similarly, the EC has participated in the JIP Management Board, in Executive Management Groups of the JIP CBRNE projects, and in expert meetings.

By involving the EDA in their advisory boards, FP7 Security Research projects are able to establish and consolidate cooperative links between the two different frameworks of CBRNE research. This is a very **important outcome** in a dual-use area. Those consulted for this case suggested that participation in advisory boards is also very important for the EDA. It provides knowledge that can be fed back into the research activities carried out within the JIP CBRNE, confirming the relevance of the effort and the mutual importance of the projects carried out.

In the specific case of the **EDEN** project, the advisory board was established to ensure that the project meets its overall objective of being end-user driven. The primary focus of the advisory board meetings is to validate the end-user requirements and to confirm that the scenarios proposed by the consortium for the three major demonstrations in RN, chemical and food contamination are aligned with these requirements. In this context, EDA is acting both as an expert in the CBRNE domain and as an end-user of the solutions developed through the project activities.

[110] SwitchProtect, MaSC, CENSIT, AMURFOCAL, RAMBO, BIOTYPE, DCLAW, BFREE, QUIXOTE, MICLID, IPODS. JIP CBRN Status Report from 02.03.2015.

[111] For further information on projects EDEN, IFREACT and MIRACLE see http://cordis.europa.eu/project/rcn/110015_en.html, http://cordis.europa.eu/project/rcn/101817_de.html and http://cordis.europa.eu/project/rcn/111244_de.html respectively.

[112] For further information on TWO BIAS, CATO, SLAM and EQUATOX see http://cordis.europa.eu/project/rcn/94832_en.html, http://cordis.europa.eu/project/rcn/102095_en.html, http://cordis.europa.eu/project/rcn/103191_en.html , http://cordis.europa.eu/project/rcn/103025_de.html respectively.

In the specific case of the **IFREACT** project, the advisory board is intended as a means of regularly (and from an early stage) bringing together industrialists and first responders, in order to facilitate adjustments and corrections to each of the activities planned within the project. The project aims at developing new CBRN protective gear for civil first-responders, which could have dual-use potential for Europe's militaries, according to the interviews. In addition to providing advice to the project, the participation of EDA in the Advisory Board has made it possible for the agency to obtain first-hand information on the solutions developed, which can be of great interest for dual-use.

F.4.3 Issues and limitations of coordination

This section reflects upon several aspects of the CBRNE research activities of the EC and/or the EDA. They do not merely concern the complementarity of the research but also point to additional facets that deserve mentioning although they do not strictly fall within the remit of this case.

First, it should be highlighted that while the EFC aims to encourage research and development, as well as the engagement of key players, it is ***not* a common framework for joint action**. The activities of the EC and EDA remain separate under the agreement, with independent frameworks, budgets, and rules. The only aspects that are shared within the EFC are the general objectives and information regarding priorities, needs, requirements and results of the projects.

Moreover, some of those consulted believe that cooperation under the EFC is hampered by the **different approaches to R&D** activities of the two organisations, with the EDA following a capability approach, and FP7 following a mission-oriented approach. More specifically, the EDA indicates what technologies and solutions are needed to cover a specific capability gap. By comparison, FP7 indicates the topic to be addressed, but not the research or technology to be used, leaving this choice to the consortia participating in the calls for proposals.

Third, the **role of the EDA within FP7 Security Research projects** has focused on providing civilian research with expert advice and opinion gained through similar activities in the military area. A closer cooperation on specific projects would not have been possible due to the differences in the programme frameworks of the EC and the EDA. As stated above, the Decision 1986/2006/EC stated clearly that the FP7 Security Research programme has a strictly civilian orientation.

Furthermore, there has been little coordination of **dissemination** activities between the EC and the EDA. This should not come as a surprise, given the strictly civilian character of the FP7 Security Research Actions and the clear target group of defence research, i.e. the armed forces of participating Member States. Consequently, the dissemination activities of FP7 funded projects focus almost exclusively on a civil security audience. Project consortia have used demonstration activities for inviting targeted audiences, such as experts in the specific relevant sector from research organisations, universities, public organisations, ministries, as well as the European Defence Agency.

To date, efforts under the EFC have focused on avoiding duplication between the activities of the EC and EDA, and on the **creation of complementarity** between their respective projects. This has, however, been limited to a rather small number of projects. Some stakeholders believe that future cooperation between the EC and EDA to coordinate research activities (i.e. in relation to H2020) would benefit from a more systematic approach. In particular, coordination could be strengthened by increasing the number of projects in which both the EC and the EDA play an advisory role (such as being part of advisory boards) and by making sure that the results obtained from projects funded under each framework feed into subsequent projects.

Finally, it is worth mentioning that in addition to the above, **several Member States pursue CBRNE-related research** on their own – in the defence realm, as well as in their civil security research efforts. The civil security research activities of Germany, Sweden and the UK serve as illustrative examples here.

- **Germany** set up its "Research for Civil Security" programme in 2007 and updated it in 2012. The focus is on solutions which guarantee the protection of the population and of critical infrastructures against threats arising from terrorism, sabotage, organised crime, piracy or the consequences of natural disasters and major accidents. In this context research

to improve protection against CBRNE hazards is of strategic importance in the German programme.

- In **Sweden**, the strategy "Research for a Safer Society" sets out the research priorities for the period 2014-18. Among the five research areas highlighted is the protection from "fire, accidents and hazardous substances (including CBRNE)".
- In the **United Kingdom** this topic has been covered since 2008 by the cross-departmental research programme "Global uncertainties: security for all in a changing world". The strategic goal of the programme is to predict, detect, prevent and mitigate threats to security, in the view that economic security depends on effective national security. The programme focuses on six core areas, of which the third is the improvement of the capabilities to fight the proliferation of chemical, biological, radiological, nuclear and explosive weapons and technologies.

The interviews conducted for this case study, as well as several stakeholder interviews undertaken as part of the wider evaluation allow for the conclusion that the CBRNE research funded by FP7 had a **positive effect** at EU and national levels, both for private and public organisations. With regard to private entities, interviews show that one of the most important results of the programme has been to promote and increase the level of cooperation between relevant organisations around Europe. On several occasions during interviews it has been stated that the same intensity and levels of cooperation would not have been possible to achieve without the FP7 Security Research Programme. In other cases, such as in the case of EDEN, one of the main objectives of a project was to create platforms and conditions for other entities and organisations to create more connections and links within the security community and increase the output of the cooperation at all levels. These findings provide an indication of the positive effects that FP7 CBRNE research had beyond those research activities that were coordinated with the EDA.

F.4.4 Conclusions and lessons learnt

This case examined the complementarity of research projects funded by the FP7 Security Research Actions, and projects overseen by the European Defence Agency (EDA), about chemical CBRNE hazards. It has shown that cooperation and coordination between the two is desirable and has been encouraged, within the limitations of their respective policies and rules.

These cross-activities have fostered **communication** between the organisations and provided opportunities for insight into the activities of the respective initiatives, enabling better coordination of strategies and solutions to common threats by: promoting civ-mil R&D cooperation between the parties; coordinating projects to avoid duplication and find coherence; and maximising complementarity among civilian security and defence-related security.

Project **dissemination** played a central role in the FP7 Security Research programme, and the results of CBRNE research were disseminated at both project and programme levels.

Particularly noteworthy is the **Community of Users** on Disaster Risk and Crisis Management, which was established by the European Commission, and which also brought together participants from all projects in the CBRNE field (more details can be found under case study 3).

Dual-use research is a highly **sensitive subject**. Further discussions at EU level may be useful to better define the ways in which the EC and the EDA can cooperate with the aim of achieving higher security levels for European citizens.

While there are a number of, partly intrinsic, limitations to the coordination of research efforts between the EC and the EDA, such as the different approaches towards R&D and the lack of a framework for a joint action, there are **significant achievements**. Chief among them is the fact that within the EFC, the EC and the EDA ensured that research efforts have not been duplicated.

Looking to the **future and H2020**, strengthening the coordination between the EC and the EDA could help to make sure that the EU develops coherent solutions, for both civilian and military purposes, and provides response capabilities to threats that do not distinguish between civil and military personnel.

F.5 Impact on the competitiveness of the European security industry

The objective of **this case study** is to assess the extent to which the FP7 Security Research Actions have contributed to the improvement of EU competitiveness and more generally to European Security Industrial Policy. It thus contributes to the evaluation of the effectiveness of the programme.

It first presents a broad overview of the challenges faced in the security sector, before going on to assess how the programme has tried to overcome these challenges. Subsequently, the case study examines four projects that have been coordinated by private industry in order to understand the impacts of these example actions and their contribution to increased competitiveness in greater detail.

The findings presented are based on evidence gathered through desk research and three interviews with private companies that coordinated Security Research projects.

F.5.1 Introduction

One of the key objectives of the FP7 Security Research Programme was to increase the competitiveness of the **European industrial security sector**.

Security has been recognised as one of the markets with the highest **potential for growth and employment** in Europe. However, there are also various challenges recognised as hampering the competitiveness of the security industry, and studies predict that the current global market share of EU security companies could decrease rapidly from 25% in 2010 to 20% in 2020 if no adequate mitigating measures are taken[113]. As a response, the security industry was made a part of the Europe 2020 flagship initiative 'An Industrial Policy for the Globalisation Era'[114].

The European security sector faces two main **challenges**: a highly fragmented market and a fragile industrial base. The European Security Industrial Policy Action Plan highlighted the need to make European companies increasingly competitive globally, but also stressed the need to improve the conditions of the EU market in order to allow European public end-users to purchase more adequate technologies with a better cost-benefit ratio[115].

One of the main challenges to competitiveness relates to the security market being **fragmented** along both national and regulatory lines. This is driven and reinforced by weaknesses that include[116]:

- The lack of standards. This relates to a lack of both common performance and technical standards, and negatively impacts on the interoperability of systems developed. Such issues were highlighted in the European Security Industrial Policy as important for increasing competitiveness;
- The absence of common approaches to security issues, policy and regulation among EU Member States;
- Low levels of EU-level cooperation and organisation within the security industry;
- Conservative attitudes of procurers and end-users in adopting new technological solutions, leading to slow take-up and implementation of novel innovation;
- The size of the security market, which may not be sufficient to offset investments in R&D needed to achieve a scale of production necessary to remain competitive.

The Industrial Security Policy Action Plan highlighted the potential for FP7 to assist in tackling the above issues, through projects relating, *inter alia*, to end-users, standardisation and interoperability, and thereby contributing to the sector's competitiveness.

[113] European Commission (2012), Commission Staff Working Paper Security Industrial Policy.

[114] COM (2010) 614 final.

[115] European Commission (2012), Commission Staff Working Paper Security Industrial Policy.

[116] Ecorys (2009) Study on the Competitiveness of the EU security industry.

F.5.2 The contribution of the FP7 Security Research theme to competitiveness

Overall, the FP7 Security Research programme has been successful in involving industrial participants. Nearly all (93%) of the FP7 Security Research projects involved at least one Private Commercial participant, including many of the leading companies in the European security industry (BAE, EADS, SAAB, SELEX-Galileo, Thales, etc.). The participant survey undertaken as part of the wider evaluation also showed that the majority (71%) of industry respondents believe that FP7-Security Research Actions have contributed to strengthening the sector's competitiveness (the comparable figure across all types of respondents was 39%).

However, several caveats to the programme's contribution to security industry competitiveness were identified through the more in-depth stakeholder interviews (see bullets below). The lack of commercialisation and low market-uptake of end-products in particular were common concerns.

- **The lack of commercialisation**. According to some stakeholders, the research actions under the FP7 Security theme are highly focused on technological development and less emphasis is put on commercialisation. To this end, much of the output of projects is of a theoretical nature. This issue is not specific to the Security Research theme, and a similar focus can be found in other themes. It also in part reflects the relatively short timeframe of FP projects (which may be insufficient to undertake both research and then commercialisation activities).
- **The low market-uptake of end-products**. In part this reflects a gap between technologies developed through the programme and real end-user needs, but there may also be other issues with market take-up. For instance, the *Study on the Competitiveness of the European Security Industry* found that one challenge to competitiveness is the need to educate end-users of the technological possibilities that exist. While the traditional defence sector is characterised by a limited number of end-users (e.g. defence ministries) with a high level of knowledge, end-users in the security sector are numerous and, individually, often lack the same breadth and depth of knowledge. This is partly due to the infancy of the market. Both challenges (misalignment and poor knowledge / awareness) have been tackled by some individual projects (e.g. with end-users in the consortium or on advisory boards) but, even so, this does not seem to be a guarantee for the market uptake of end-results. For example, end-users may welcome the possibility to participate in a demonstration project, but this is not a guarantee that they will ultimately purchase the associated technology.
- **The long time to market.** Interviewees suggest a time gap of 18-24 months from call to start of a project is not unusual, and then the projects themselves may last several years. This is a very long time from the perspective of industry and the market, in which demands and conditions may change, and the relevance of project objectives and outputs may reduce as a result. This point was also highlighted in the FP7 Interim Evaluation, which stated that the relatively long time spans of project development were more appropriate for basic research than near-market applications.
- **Difficulties involving Intellectual Property Rights (IPR)**. Complex rules around IPR can inhibit products being developed from project results, while many industrial actors do not want to share innovation with other consortium partners for reasons of competition.
- **The on-going national preference.** The multi-national approach in FP7 can make the end-results of projects less marketable to end-users and procurers in a market that is heavily fragmented along national lines. For example, one interviewee put forward the example that a national police force might be reluctant to buy technology developed by consortia encompassing companies from several EU Member States.

It may, however, be important to make a **distinction between short-term and medium- to long-term impacts** of the FP7 Security Research Programme, as some stakeholders have argued that the most important outcome of the FP7 Security Research Actions – helping to make companies, and the European market as a whole, competitive – does not necessarily require the direct uptake and exploitation of the project outputs (products) themselves. Instead, companies are using the programme for incremental rather than disruptive innovation. Indeed, it emerges from the interviews that the knowledge, cooperation and networking stemming from FP7

Security research projects are equally important assets for competitiveness. However, their impact on the security sector may only materialise on a longer term-basis.

- So, for example, most respondents (85%) to the participant survey found that the FP7 Security Research Programme had made a substantial contribution to its '**capability building**' objective. This is in line with the findings of the Interim Evaluation, which stated that one of the main reasons for larger companies to participate in the Programme was the possibility for cooperation.
- In terms of the Programme's contribution to the **EU's global competitiveness**, some stakeholders have argued that many projects have attracted attention outside the EU, illustrating that FP7 has helped increase the EU's standing globally. In addition, FP7 has opened up market opportunities for smaller countries to participate in large-scale projects, something that would not have been possible at the national level.

In summary, the FP7 Security Research Actions have so far resulted in a relatively low level of commercialisation of end-results, but have achieved more wide-spread and important immaterial outcomes, such as from cooperation and networking, or through the opening up the market for actors from smaller countries.

F.5.3 Projects coordinated by an industrial participant

This section examines four example projects that have been led (coordinated) by a participant from the Private Commercial sector (i.e. industry), and explores their approach to enhancing the competitiveness of the security market or to increasing the market-readiness of their outputs.

The example of PROTECTRAIL[117]

Project Title	PROTECTRAIL: Railway-Industry Partnership for Integrated Security of Rail Transport
Project Code	242270
Project type	CP - Collaborative project (generic)
Start-end dates	2010-09-01 / 2014-06-30
Coordinator	ANSALDO STS

The overall focus of PROTECTRAIL was **tackling railway security** from the perspective of a layered integrated system, and it aimed to provide tools and strategies for evaluating the security potential of a given security sub-mission, in terms of performance, reliability, speed and costs. Outputs from the project included the definition of user requirements and the development of systems architecture mechanisms required to respond to well-known needs for rail protection. This system was tested through simulations in France, Italy and Poland. So far the application of results appears to be limited but project participants report that the project did lead to enhanced capabilities, which will provide competitive for those involved the project.

One of the observations made in project stakeholder interviews related to the changing and unpredictable market demands pertinent to the security industry. The project participants invested in R&D in the railway security sector due to the then prevailing **market conditions**, which indicated that there would be heightened demand for security solutions. However, at the end of the project this surge in demand and investment by public authorities had not materialised.

One of the main **demand drivers** in the security sector is the perception of security threats. Demand is thus influenced by new 'events' such as terrorist attacks. Since such specific 'events' are by their very nature largely unpredictable, the pattern of demand over time can be extremely uncertain[118]. However, the project made concerted efforts to ensure the potential for market uptake by involving the main railway and security solutions suppliers, research groups, and major railway operators (under-takings and infrastructure managers). This guaranteed that project solutions would satisfy user needs. However, in light of decreased market demand for railway security systems, the end-product of the project had lost some of its market relevance.

[117] http://cordis.europa.eu/project/rcn/95607_en.html

[118] Ecorys (2009) Study on the Competitiveness of the EU security industry.

The **lack of standards** and a common European approach to security in the railway sector were identified as major barriers to competitiveness by the project. A common approach to security, both in terms of performance standards and public policy, would make it easier to bring products to market, especially in view of unpredictable demand patterns. This would help foster a stable demand for security products and services without running the risk that the products become out-dated. Interviewees suggested that the issues of common approaches and standards have still not been sufficiently tackled through the Security Research programme.

The example of ARCHIMEDES[119]

Project Title	ARCHIMEDES: Support to Security end-users
Project Code	285061
Project type	CSA-SA - Support actions
Start/end date	2012-01-01 / 2014-12-31
Coordinator	EOS scrl

The strategic goal of ARCHIMEDES was to **overcome the cultural, practical, economic, social and legal barriers** that hamper the exploitation of research and development results in Europe. Its strategy was based on the enhancement of end-users' and operators' ownership of all stages of the European research process, and therefore making European research more end-user oriented.

The approach was based on the recognition of a **need to increase end-users' awareness and understanding of their innovation needs**, and their ability to assess, define, and revise their operational procedures and capability gaps. By designing tools that allow end-users to analyse their needs and the technology options available, the project hoped that the take-up of innovative technological solutions by end-users would be made easier and less costly.

The ARCHIMEDES' **approach** was also intended to bring end-users and the research community closers to each other, creating a more structured dialogue around research needs in the security sector. This was based on the fundamental idea that closer cooperation on security research needs to be end-user driven, with a clear focus on the definition of their operational needs; and that this makes it possible to achieve the strategic policy objectives set out at EU level in terms of security policy.

The ARCHIMEDES project was therefore based on the **concept** that the take-up of the outputs of research and development processes can really only happen if they are the result of a concerted action between end-users (the actual operators that will deploy a particular system, technology, product or solution) and the research and commercial communities.

The ARCHIMEDES project **demonstrated** that a fundamental part in this process is the enhancement of end-users' awareness of the importance of defining their operational requirements from a research and innovation point of view. This, in turn, is made possible only through close cooperation with those organisations that can actually provide that research and development, supporting end-users in understanding the innovation potential, as well as the future developments of specific technology domains.

The example of SECURECHAINS[120]

Project Title	SECURECHAINS: Integration of Security Technology Supply Chains and Identification of weaknesses and untapped potential
Project Code	242417
Project type	CSA-SA - Support actions
Start / end date	2010-05-01 / 2012-04-30
Coordinator	Inovamais - Servicos de Consultadoria em Inovacao Tecnologica s.a.

SECURECHAINS sought to contribute to the creation of a **more competitive Security Technology Supply Chain** (STSC) through the increased integration of business processes between enterprises across the entire supply chain. It sought to achieve this through defining, adopting, testing and validating a methodology to support European organisations to achieve higher integration within the STSC.

[119] http://cordis.europa.eu/project/rcn/101736_en.html

[120] http://cordis.europa.eu/project/rcn/94425_en.html

One factor identified by the project as having a **positive impact** on the effectiveness of the STSC was the identification, stimulation and exploitation of research and innovation results and capabilities available in Europe.

The main **achievements** of the project have included:

- Awareness-raising among 2,500 SMEs, large companies, RTOs and other STSC stakeholders about EU RTD funding programmes;
- The development of a technology screening activity at European level to identify weak spots in the security supply chains;
- The development of nine technology trees in order to exemplify the main actors in important Supply Chain Technologies;
- The identification of the problems that inhibit the participation of SMEs in European RTD activities;
- Interviews and on-site visits with 120 SMEs and RTOs, to collect data on research capabilities and technology acquisition needs;
- The organisation of three communication exchange fora at European Security related events;
- Screening of the best 20 new RTD proposal ideas emerging from the on-site visits;
- The provision of guidance and technical assistance to STSC actors, especially SMEs, so that they are able to present successful proposals to FP7;
- The creation of a communication platform / website / database of security actors and stakeholders allowing the exchange of information and facilitating networking among major STSC stakeholders.

The example of OSMOSIS[121]

Project Title	OSMOSIS: Overcoming Security Market Obstacles for SMEs Involvement in the technological Supply chain
Project Code	242416
Project type	CSA-SA - Support actions
Start / end date	2010-04-01 / 2012-03-31
Coordinator	CIAOTECH Srl

The main objective of the OSMOSIS project was to **foster the involvement of SMEs in the security technology supply chain**, facilitating the collaboration between SMEs and the key stakeholders in the European security domain (system integrators, end-users and technology providers). The project aimed to create a nurturing environment for the involvement of SMEs in the overall security market, through the design and development of the following services:

- A database of relevant SMEs
- A database of RTD project ideas to encourage collaboration between organisations
- A list of research opportunities, in the security field, that could be exploited by SMEs to collaborate with large organisations
- Information on security-related grants
- Interactive communication tools to allow the communication of the identified opportunities and the transfer of knowledge among registered users.

The **logic behind this approach** to increasing the competitiveness of the security market is based on the establishment of a centre of reference for organisations involved in the Security Market chain, where information on projects, investments, requirements, technological trends, project ideas and competences could be shared and promoted. The support to SMEs with

[121] http://cordis.europa.eu/project/rcn/94249_en.html

specific capacities and capabilities has turned out to be of strategic importance, in order to give them visibility and increasing their access to new opportunities both within the programme and on the market.

F.5.4 Conclusions and lessons learnt

A core obstacle to achieving a fully competitive security market in the EU is its fragmentation, which is caused by:

- **A lack of standardisation** at technical level. Purchasing bodies follow national procedures and base their requests on specific needs and requirements. The presence of different technical requirements and procedures hampers the possibility for companies to operate in a single market;
- **The absence of common approaches** to security issues, policy and regulation among EU Member States;
- **Low levels of EU cooperation** and organisation within the security industry;
- **Conservative attitudes** amongst procurers and end-users towards adopting new technological solutions, leading to a slowdown in the take-up and implementation of novel innovation.

One of fundamental objectives of the FP7 Security Research Programme was to tackle these issues and to support the establishment of a more competitive market for security solutions, products, systems and technologies.

The response and active participation of private companies to the opportunities presented by the programme has been in itself a success, with more than 90% of the project consortia including at least one private commercial organisation. However, the programme's contribution to competitiveness did not always meet the expectations of businesses. The causes identified are at programme level, deriving from the structure of the programme and the way it has been implemented. These include:

- **A lack of commercialisation**. Projects funded through the FP7 Security theme have focused on technological development more than on the commercialisation of the outputs and their operational use. This was encouraged by the way in which calls for proposals and work programmes identified the key topics and priorities, as well as by the overall set-up of FP7 (e.g. project timeframes);
- **A low level of take-up of project outputs.** Technical requirements are often developed by the research community instead of being specified by the operators, leading to final products that are not well aligned with real demand. There is also low-level awareness and knowledge about existing solutions within the sector;
- **The long time to market.** The lengthy FP process (from definition of work programmes to project completion) can reduce the eventual relevance of results;
- Complex rules around **IPR** inhibit products being developed from project results;
- Different national **standards** are applied resulting in high market fragmentation.

Some projects led by private companies were focused on trying to identify and deploy solutions to these barriers. These have shown that:

- Strong interaction with end-users can increase the marketability of final products (although this is not a guarantee e.g. due to the unpredictable nature of demand);
- Projects with industry coordinators and partnerships tend to pay more attention to the exploitation phase;
- SME involvement in EU research projects can be increased and incentivised by providing fora in which to share experiences and showcase their capabilities;
- Standardisation of procurement procedures and requirements could help create opportunities for commercial companies across Europe.

It is worth noting that Commission is also trying to address demand side fragmentation, for instance through increasing support for groups of public procurers who work together on joint Pre-Commercial Procurements (PCP). These actions have raised awareness, encouraged cooperation among public procurers from different Member States and led to jointly implemented pre-commercial procurements.

This support is being extended under Horizon 2020 (H2020), with financial incentives such as the PCP Co-Fund actions available for consortia of public procurers working together on joint PCPs. One topic for PCP proposals has been included in one of the first calls for proposals under the secure societies challenge area of H2020.

Under Horizon 2020, the Commission will also co-fund groups of procurers to undertake joint Public Procurement of Innovative solutions (PPI) actions. This is intended to speed up the development of innovative solutions by encouraging cooperation between procurers from across Europe.

At the workshop undertaken as part of the wider evaluation, these new public procurement instruments were broadly welcomed as a means to start tackling fragmentation on the demand side.

Lessons learnt for H2020

From the interviews and the analysis of the information gathered, it emerges that in order to increase the competitiveness of the security market in the EU, some fundamental steps should be taken:

- Actions under the H2020 should be further focused on strengthening common approaches and standards;
- More focus should be given to the marketability and commercialisation of project results, even at the proposal stage;
- More emphasis should be placed on networking and understanding end-users' operational needs, even before the proposal stage. The European Commission could play a facilitating role in this regard.

F.6 Productive Use of IPR from Security Research Actions

This case study examines the use of IPR within the FP7 Security Research programme, and in particular the way IPR issues have been tackled and managed by project consortia. It focuses particularly on the achievements and experiences of a small number of research projects that have specifically led to patents as an output. Looking at the potential use and dissemination of results through IPR, the case study contributes to the evaluation of the effectiveness of the programme with respect to the development of the security market.

Following an introduction to the issue and scope treated, the case study examines the place of IPR within the FP7 Security Research Programme and the IPR outcomes from the programme, before presenting the conclusions and lessons for Horizon 2020.

The research carried out for this case consists of documentary analysis, interviews with 5 experts from the European Commission, the IPR Helpdesk and three external organisations participating in the FP7 Security Research programme. Finally, the case draws on data from the Commission's SESAM project monitoring database.

F.6.1 Introduction: the issue and scope

Intellectual Property Rights (IPR), as defined by the World Intellectual Property Organisation (WIPO), are "the rights to use and sell creations of the mind: inventions, literacy and artistic works, and symbols, names, images, and designs used in commerce". Intellectual property (and IPR) therefore covers patents, utility models, industrial designs, copyrights, geographical indications and service marks, etc.

IPR systems play a significant role in the innovation process and in the quest for competitiveness. IPR is used for protecting the investments of innovative players against potential copycats, and is a key incentive to undertaking risky investments in the first place[122]. IPR is also important for research, and for the dissemination, exploitation and use of research results. IPR can be a prerequisite for intellectual assets to emerge in markets, and to turn research results into marketable products.

Promoting the **use and dissemination of FP project results** was a key objective of FP7[123], and efforts have been made to raise awareness of the value and importance of intellectual assets, as well as the necessity to secure and manage them. In particular, participants in the programme have been strongly encouraged to consider and tackle IPR issues as soon as possible during the preparation of projects, insofar as IPR issues can affect the way the projects are conducted or the exploitation of results afterwards.

The Commission has also been committed to **improving IPR management** in research projects, and has attempted to clarify and simplify IPR provisions (especially terms and conditions) in FP7 compared with FP6. For instance, a guide to Intellectual Property Rules for FP7 projects was produced, covering the various issues and potential pitfalls that participants may encounter when preparing and participating in an FP7 project. An IPR Helpdesk initiative was also implemented to assist FP7 participants in understanding underlying principles to IPR in research projects.

[122] United Nations Economic Commission for Europe (2011) Intellectual Property Commercialization – Policy options and practical instruments.

[123] Decision 1982/2006/EC.

FP7 Security research projects often produce results (or 'foregrounds'[124]) that can be sensitive or even include classified data and information. Therefore, specific rules have been established to govern the use of IPR in this field, and specific rules apply for the handling of classified information[125].

Projects funded through the FP7 Security Research Actions have already led to the production of IPR, and in a small number of cases specifically to new patents.

F.6.2 IPR within the FP7 security research programme

Before the establishment of the FP7 Security Research programme, the **GoP report** (2004)[126] noted that one of the issues in establishing such a programme, was that (previous) Framework Programmes did not offer the necessary conditions for 'secured' research in terms of confidentiality, IPR and funding. It concluded that in order to make a European Security Research programme work, it must be flexible and take into account the specific nature of security research. In particular, the Commission should develop the necessary rules for IPR within the programme.

The **ESRAB** report (2006)[127] reiterated that for European security research to be undertaken successfully, the programme must address and make provisions for the specificities and sensitivities of implementing European security research, including reinforcing the protection of intellectual property rights.

Subsequently, the EC '**Guide to Intellectual Property Rules** for FP7 projects' (v3) includes some specific provisions that relate to security research projects alone. For example, a simplification introduced in FP7 (overall) is that, subject to prior agreement by all participants in a project, one partner can be authorised to transfer the ownership of any foreground it generates to a specific third party (e.g. mother company or affiliate). Also, once such a global authorisation has been provided, the participant no longer has to give prior notice to other participants of each individual transfer, and the other participants no longer have the possibility to object. **In security research projects** however, the IPR guide states that such transfers to third parties should "continue to be decided on a case-by-case basis", and should be "handled with the greatest caution".

The guide further states[128]: "*In order to protect the participants and to make sure that the relevant national, Community or European Union and – if relevant international - rules on handling such data or information are respected by the participants, the dissemination of foreground can be limited to specific participants or purposes.*

Upon the decision of the participants – in agreement with the Commission – the dissemination of foreground subject to such legal restrictions can be extended to third parties which are not part of the consortium.

Due to the sensitive character of classified information and data, special clauses may be inserted in security research projects which – as a general rule – exclude the dissemination of foreground to parent and/or affiliate companies or any legal entity which does not form part of the consortium. The exception hereto is allowed, but only upon a joint decision of participants and Commission, taken on a case-by-case-basis."

[124] As stated in the FP7 Participation Rules (Regulation 1906/2006/EC) " [to] 'foreground' means the results, including information, whether or not they can be protected, which are generated by the indirect action concerned. Such results include rights related to copyright, design rights, patent rights, plant variety rights or similar forms of protection".

[125] The classification of information is solely based on the content of the information. Framework Programme projects that include EUCI (European Union Classified Information) have to follow the rules for protecting EUCI (Commission Decision 2015/444 on the security rules for protecting EU classified information).

[126] Group of Personalities in the field of Security Research (2004) Research for a Secure Europe.

[127] European Security Research Advisory Board (2006) Meeting the challenge: the European Security Research Agenda.

[128] http://ec.europa.eu/research/participants/data/ref/fp7/89593/ipr_en.pdf

F.6.3 IPR outcomes from the FP7 Security Research programme

As of the end of December 2014, 102 FP7 Security research projects had submitted final reports and 61 of these had been processed, with all outputs recorded within the Commission's **SESAM project monitoring** database. This partial dataset, comprising projects from the earliest calls and those of shorter duration, nonetheless allows some insight into the wider set of 300+ projects funded through the programme.

SESAM data provides information on the production of '**foregrounds'**. These are tangible and intangible results (including information and knowledge) that are generated in a project, regardless of whether or not it can be protected[129]. There are 10 FP7 Security Research projects (16% of 61 assessed) that have reported the generation of at least one foreground (22 separate foregrounds between them). These include:

- The commercial exploitation of R&D results (9 of 61 projects);
- The exploitation of results through (social) innovation (5);
- The exploitation of results through EU policies (3);
- The general advancement of knowledge (1).

The proportion of projects reporting foregrounds in the Security Research programme (16%) is slightly higher than seen in FP7 overall (13%[130]).

Intellectual property rights are one sub-set of foregrounds, and SESAM provides separate information on the generation of IPR[131] amongst the projects assessed. It shows that, as of December 2014, there had been seven Security Research projects (11% of the 61 assessed) – spread across 5 mission areas – that had reported at least one IPR. All of these projects originated from the first FP7 Calls in 2007, though from a variety of different programme areas, and addressing very different topics. Between them, the seven projects generating IPR reported a total of eleven intellectual property rights of different types, including nine patents, one utility model, and one copyright[132].

The Security research projects reporting IPR (and the specifics of the IPR reported) are detailed in the table below. Most of these are technological research projects, involving a strong industrial base and potential end-users. Most are market oriented in nature, with some form of commercialisation plan. For example:

- SECRICOM involved a large range of potential customers in its activities;
- IDETECT4ALL involved industrial players and end-users. It set up a business model and undertook business evaluations of the system it developed. It identified potential clients, competitors and alternative product providers that might be of relevance, and it set up a financial plan for further commercialisations (covering potential clients, potential market growth, scenarios, forecasts, etc.);
- INFRA created good connections with end-users, which enabled the dissemination of results and aroused the interest of potential customers.

[129] Such results include rights to related copyright, design rights, patent rights, plant variety rights, and similar forms of protection.

[130] FP7 Monitoring Report 2013, based on the 7,288 projects with a submitted and processed final report, as at 1 December 2014.

[131] Defined here as legal rights aimed at protecting the creation of intellect, such as inventions, appearance of products, literary artistic and scientific works and signs, among others.

[132] One of these projects is in fact shown within SESAM as reporting 9 IPRs. However, other than one patent, it seems that the other cases of IPR reported in fact relate to *potential* opportunities to exploit this patent. As such, only one reported IPR from this project is included within our analysis.

Table 44: FP7 Security Research projects reporting IPR

Activity / Area	Project acronym and title	Project topic	IPR description
Security of infrastructures and utilities	IDETECT 4ALL: Novel Intruder Detection & Authentication Optical Sensing Technology	Small area 24 hour surveillance	• Utility model - Smart multi sensor
Security of citizens	LOTUS: Localisation of Threat Substances in Urban Society	Localisation and tracking of components of substance production	• Patent - Differential Mobility Analyser
	COCAE: Cooperation across Europe for Cd(Zn)Te based Security Instruments	Stand off scanning and detection of hidden dangerous materials and/or stowaways,	• Patent - Method of Radiation Detector Formation • Patent - Method of fabrication of X- and γ-ray detectors • Patent - Method of surface doping of semiconductor compounds with group III elements
Intelligent surveillance and border security	TALOS: Transportable Autonomous patrol for Land Border Surveillance	Unregulated land borders surveillance system	• Copyright - Mobile Network Clock Synchronisation Software
Restoring security and safety in case of crisis	SECRICOM: Seamless Communication for Crisis Management	Wireless communication for EU crisis management	• Patent - Apparatus for calculating a result of a scalar multiplication • Patent - System for safe infrastructure for mobile agents and grid clusters • Patent - Cryptography processor, smart card and method for calculating a result of an exponentiation
Security systems integration, inter-connectivity and interoperability (ICT-SEC)	INFRA: Innovative and Novel First Responders Applications	ICT support for first responders	• Patent - An analysis method and system for blood
	ISTIMES: Integrated System for Transport Infrastructures surveillance and Monitoring by Electromagnetic Sensing	Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures	• Patent - New lost cost measurement system for Long term Monitoring (i.e. infrastructures, buildings,...)

Source: Technopolis analysis of SESAM database - 2007 Work Programme

Compared to the **Cooperation Specific Programme** overall, the reporting of IPR in the Security Research programme is relatively low. As the figure below[133] shows, the proportion of projects reporting IPR in the Security Research programme (11%) is lower than seen in the FP7 Cooperation Specific Programme overall (19%), while the number of IPRs reported per project (0.3) is also around half the average rate (0.5).

Table 45: IPR reporting across the FP7 Cooperation Specific Programme

Programme	Final reports assessed	% of projects reporting at least one IPR	IPRs reported per project assessed
NMP	350	40%	1.1
Energy	105	31%	0.9
Health	400	25%	0.7
KBBE	185	18%	0.5
Transport	280	11%	0.3
Security	79	11%	0.3
Environment	216	7%	0.1
JTI	121	7%	0.1
Space	111	6%	0.2
SSH	131	0%	0.0
Other	11	9%	0.3
Cooperation Programme	**1,989**	**19%**	**0.5**

Calculated from the FP7 Monitoring Report, 2013

[133] Calculated from data presented in the FP7 Monitoring Report 2013, based on final reports submitted and assessed as of 1 December 2014

Available data therefore suggests that only a small proportion of all FP7 Security Research projects will generate IPR by the time of their completion, which may (once all final reports have been submitted and processed) equate to some 30-40 projects in total, and 50-60 IPRs being reported (often as patent applications).

While this is below the rate seen across the Cooperation Specific Programme as a whole, there is no clear basis for determining if this is high or low for FP7 Security Research specifically. Certainly one would not expect all projects in the programme to result in IPR, including for example those projects that are less applied in nature, or those within certain parts of the programme (e.g. many of the projects in the security and society domain). However, given the largely applied, near-term nature of much of the Security Research programme, it is perhaps surprising that more projects are not reporting IPR.

The comparably low level of exploitation and patents for FP7 Security Research may be a result of the strategy to focus the SRAs more on integration than on the technologies needed for security applications that may exist already.

Another possible explanation is that the security industry tends to protect results (and particularly in the short term) by **means other than IPR**. Commercialisation can be a long process, which rarely occurs at – or immediately after – the end of an FP project. Even if the research results are expected to eventually find commercial application (e.g. through licencing), to get to this point will often require additional investment, work and time. The relatively high cost of maintaining IPR (through e.g. patents) whilst new technology is still at an early stage of development, means project partners might not immediately rush to address IPR protection.

Often projects will result in proven concepts, rather than marketable products. Most of the time, at the end of a project, industrial players **need further steps** and additional investments before their results can be marketed. Quite often, one research project is the basis for another one, and marketing can be expected after two or more FP projects. For instance, even though the SECRICOM project successfully achieved a proof of concept, the prototype was not ready for application immediately after the project. The knowledge and IP generated by the project have instead been transferred to another FP7 project[134]. A comparable situation exists for project EMPHASIS that took off from the LOTUS project, both complemented by project BONAS. In the IDETECT4all project, the coordinator patented basic sensor technology before the project started, following an earlier UK project.

The dispersal of IP across the consortium, and a **lack of central control and awareness** of outcomes, may also reduce the generation of IPR, or at least the rate at which it is reported to the Commission. In the Security Research projects listed above, each IPR reported is filed by only one of the partner organisations. This is because most of the time foregrounds are generated by individual partners (rather than jointly by several members of a consortium), and are therefore owned by a single partner. It is then down to the individual partner to make use of, protect and exploit this IP as they wish. So, for example, the SECRICOM project allowed at least five partners to develop new products and services, yet only one partner has so far patented their outputs. Often partners are not even aware of IPR activities conducted by other members of the consortium. Therefore, it is possible that some project partners may have used their foreground acquired during the project for their own products or services, but this is not visible and known by other consortium partners. Similarly, IPR as reported in the project final report, may only represent a proportion of the real situation.

There seems to be a discrepancy between the commitment of the Commission to reinforce the IPR management in research projects and the actual change in project partners' behaviour within the Security Research programme. Indeed, despite the attempts to increase awareness of the importance to establish a clear agreement regarding the ownership and use of IP at an early stage of the projects, this issue is not yet well integrated and understood by all participants.

[134] The IP was transferred to the FREESIC project http://cordis.europa.eu/project/rcn/102280_en.html.

IPR is also commonly seen as too **complex and costly** to tackle, particularly amongst academic partners, who do not have dedicated and competent staff in this area. Others lack the knowledge, skills and experience (and sometimes the incentives) to address questions of IPR management and the negotiation of IPR rules. Even for some industrial partners (particularly SMEs), IPR is not an integral part of their overall business strategy. The investment in the production of IPR can be too costly for the companies, in so far as developed technologies become obsolete too quickly.

There can be a **mismatch between the interests of different project partners** – and particularly between academic and industrial partners – as well as competition between different industrial participants. It can be difficult to reconcile respective interests, and particularly a desire to disseminate knowledge, and a desire to protect it (which can be made more difficult by the dissemination).

While general guidance has been produced on IP issues for project consortia, reaching an agreement on IP sharing arrangements can be complicated – and situations can arise where partners refuse to share information with other members of the consortium for competition reasons.

F.6.4 Conclusions and lessons learnt

Those interviewed for this case suggest that for a project to result in the production of IPR, a number of conditions must be met, amongst which the most important are:

- **Patents or other forms of IPR** can be produced only if knowledge transfer and IPR management are clearly defined – and procedures and rules for IPR management are set out before a project starts. IPR possibilities should be assessed at a very early stage so that successful marketing can occur, and a clear and strategic structure to handle intellectual property is essential.
- Consequently, consortia should be encouraged to develop structures and **commercialisation** plans that distinguish between dissemination of findings and application of achieved development. Consortia should also be encouraged to devote more time to dissemination and exploitation activities.
- **Participation of industry** is important for the generation of IPR outputs and the application of project results. The presence of industrial partners within a consortium that have a direct interest in marketing project results appears to be a determinant of success. Indeed, industrial partners are likely to sell resulting products, and could ensure the new technology protection. They could also ensure that project design and execution remain focused on operational results.
- A more extensive **awareness and understanding** of the importance and management of IPR issues among partners is important – particularly amongst academic participants.
- A **legal framework** is of the utmost importance, but as long as participants do not have any effective know how to manage IPR properly, difficulties will remain. A lack of understanding and a lack of professional management of IPR could dissuade industry from participating in collaborative research projects, as well as cause potential conflicts during the projects and the limited application of results.

Various initiatives have been carried out in order to improve knowledge transfer and IP management capabilities, including the Recommendation[135] on the "management of intellectual property in knowledge transfer activities and Code of Practice for universities and other public research organisations" produced by the European Research Area Committee's (ERAC) Knowledge Transfer Working Group, and endorsed by a Council Resolution in May 2008.

[135] Commission Recommendation C(2008)1329.

Despite those initiatives, IP management is still a problem. Indeed, raising awareness is a long-term process. It takes time to educate knowledge transfer and IPR professionals, and to set up professional support structures. It is of high importance to intensify the process of professional development of knowledge transfer and IPR management. In this regard, it is essential to keep developing the capabilities of the FP7 (and Horizon 2020) security research project consortia to deal with IPR issues.

The **Commission Guide to Intellectual Property Rules** for FP7 Projects can increase understanding of IP use, in particular for organisations that lack internal resources to get accurate information on IP rules without any professional support (for instance SMEs). Therefore, such initiatives should be repeated in order to promote a better awareness of IPR issues. The reinforcement of the role of the European IPR Helpdesk to provide participants with clear advice in relation to IPR seems to be a crucial point. Professional management of IPR issues within consortia could also be addressed through the association and support of various national patent agencies as well as the European Patent Agency.

F.7 Demonstration projects

This case study considers the role of demonstration projects within the FP7 Security Research Programme and explores the extent to which they have been successfully deployed to promote the application of innovative security solutions. It contributes to the evaluation of the achievements and European added value of the programme.

The case begins by providing some background to the inclusion of demonstration projects within the FP7 Security Research Programme, before explaining the two-phase approach employed to their implementation. It goes on to introduce the 14 demonstration projects funded and undertaken over both phases, looking at their objective, activities, outputs and achievements. Finally, the case highlights several issues and limitations, before drawing conclusions and lessons for the future.

The research conducted in the development of the case included document analysis, semi-structured interviews with four experts (from the Commission and consortium partners in five of the Demonstration Projects[136]) and the analysis of CORDA data.

F.7.1 Introduction

Fourteen **Demonstration Projects** were funded through the FP7 Security Research Programme. These were intended as flagship initiatives of the programme, integrating a number of systems to achieve multi-mission objectives in selected areas of significant European interest. This section sets out the origins of these projects.

Origins of Security Demonstration projects

From an early stage, demonstration activities were seen as an integral component of FP7 Security Research Actions. **ESRAB**[137] highlighted that the successful achievement of demonstration programmes would be dependent upon the coherent, compatible and synchronised development of capabilities and system/technology building blocks. In relation to demonstration programmes, the ESRAB report explained further that "*for large security solutions to enter into service, numerous independent but interrelated systems must be integrated and then demonstrated to prove operational effectiveness… These European flagships would aim to ensure the coherent development of the required system building blocks, architectures and standards*".

ESRAB proposed a series of five demonstration programmes in areas of significant European interest that offered high potential to deliver European added value:

- Aftermath crisis management;
- European-wide integrated border control system;
- Logistic and supply chain security;
- Security of mass transportation;
- Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE).

So as to ensure that each demonstration programme is clearly described in terms of the required capability and system building blocks, ESRAB also recommended that **support activities** be first awarded, which would define the strategic roadmaps required for each demonstration programme. These would take into account completed, on-going and planned work, and lay out the further work required.

These recommendations from ESRAB - the concept of demonstration programmes, the five areas of focus, and the preliminary support activities - were all deployed through the FP7 Security Research Programme from its first year of operation.

[136] Some interviewed experts participated in more than one demonstration project.

[137] European Security Research Advisory Board (2006) Meeting the challenge: the European Security Research Agenda.

Calls for Demonstration Projects

The initial **(2007) work programme** for the FP7 Security Research theme explained the ambitions and architecture of the programme, including the central role of demonstration projects in achieving mission objectives.

It highlighted that "successful demonstration of the appropriateness and performance of novel solutions is a key factor for the take-up of the output of the research work and its implementation by security policies and measures", and that therefore its demonstration projects would be "the **flagships** of the Security theme."

Demonstration projects would "carry out research aiming at large scale **integration, validation and demonstration** of new security systems of systems, going significantly beyond the start of art", and would "depend upon the compatible, complementary and interoperable development of requisite system and technology building blocks of the integration projects and capability projects".

Given that demonstration projects were intended to promote the application of innovative solutions, this also implied "strong **involvement of end-users**", taking account of relevant legal and societal issues, and with strong links to standardisation.

Finally, the work programme explained that – following the recommendations of the ESRAB report - demonstration projects would be implemented in **two phases**:

- **Initial (Phase I) projects**: would take the form of short (1-1.5 year) coordination and support actions. They would both define the strategic roadmaps for the next phase of demonstration, and ensure EU-wide awareness of the initiative amongst relevant stakeholders. The roadmaps would take into account relevant completed, on-going and planned work, and indicate further research needs for integration and capability projects within the programme (and beyond).
- **Subsequent (Phase II) projects**: would then technically implement the system of systems demonstration projects, taking account of steps that must follow the research, such as standardisation, development of marketable products and procurement. These collaborative projects would mobilise a significant volume of resources, typically last 4 years, and have significant involvement from industrial partners and end-users. They would demonstrate the efficiency of solutions and help to create an EU-wide market for them.

Calls for demonstration projects were launched gradually over the course of FP7. The Security Call 1 (2007) launched two Phase I demonstration projects, relating to mass transportation (within the 'security of Infrastructures and utilities' mission area) and border management (in the 'intelligent surveillance and border security' mission area). The call also noted that in parallel, novel and improved technologies would be developed, adapted and integrated into systems through other integration and capability projects, in order to be ready for the next generation of integrated security systems of systems to be demonstrated in the future.

A further four calls for Phase I demonstration projects were launched in the subsequent 2009 and 2010 work programmes (see the table below). The call for Phase I crisis management projects was issued in 2009 and again in 2010, as no proposals were selected from the first round. The first two calls for Phase II projects appeared in the 2010 work programme, with a further three calls appearing in 2012 and 2013.

Table 46: Calls for Phase I and II demonstration projects

	Work programme					
Mission area	**2007**	**2009**	**2010**	**2011**	**2012**	**2013**
Increasing the security of citizens		Ph I: Logistics & supply chain Ph I: CBRNE			Ph II: CBRNE	
Increasing the security of infrastructures and utilities	Ph I: Mass transportation		Ph II: Mass transportation			Ph II: Logistics & supply chain
Intelligent surveillance and enhancing border security	Ph I: Border management		Ph II: Border management			
Restoring security and safety in case of crisis		Ph I: Crisis management	Ph I : Crisis management (re-launched)			Ph II: Crisis management

Selected Demonstration Projects

From the series of calls for proposals, a total of **14 demonstration projects** were selected during the course of FP7, including nine Phase I projects and five Phase II projects. This relatively small number is consistent with the objective to integrate into large-scale projects the outputs and outcomes from capacity and integrated projects, and to concentrate funding on a limited number of flagship projects.

The distribution of demonstration projects across the Security Research Programme's **mission areas** is shown in the table below. The largest number took place in the 'Restoring security and safety in case of crisis' area, which accounted for five of the nine Phase I demonstration projects. Only one Phase II project took place in each area, with the exception of 'infrastructure and utilities', where there were two.

Table 47: Distribution of demonstration projects by mission

Missions	**Phase I**	**Phase II**	**Total**
Increasing the Security of citizens	2	1	**3**
Increasing the Security of infrastructures and utilities	1	2	**3**
Intelligent surveillance and enhancing border security	1	1	**2**
Restoring security and safety in case of crisis	5	1	**6**
Total number of demonstration projects	**9**	**5**	**14**

Source: CORDA data (Feb. 2015)

The distribution across **topics** (which relate to the ESRAB recommended focus areas for five demonstration programmes) is shown in the following table. The number of Phase I projects in each of these topics varied between one and three, but only one Phase II project took place in each thematic field, as was intended.

Table 48: Distribution of demonstration projects by theme

Themes	**Phase I**	**Phase II**	**Total**
Aftermath crisis management	3	1	**4**
CBRNE	2	1	**3**
Integrated border control and management	1	1	**2**
Logistic and supply chain security	2	1	**3**
Security of mass transportation	1	1	**2**
Total	**9**	**5**	**14**

Source: CORDA data (Feb. 2015) and Work Programmes 2007-2013

The table below summarises the basic **characteristics** of the funded Phase I and II demonstration projects, and highlights clear differences between the two:

- The Phase I projects were much smaller in **size** (€1m in EC contributions per project on average) than the average FP7 Security Research project (€4.1m), while Phase II demonstration projects (€28.2m) were considerably bigger.
- The large **number of partners** in Phase II projects is intrinsic to this type of activity and the need to integrate a large number of solutions (from industrial partners) as well as different types of end-users: first responders, crisis managers, national/European agencies, policy makers, etc. within the activities.
- While Phase II projects are similar in **duration** to the average Security Research theme project, the Phase I projects tend to be much shorter.

Table 49: 'Typical' characteristics of Phase I and II demonstration projects

	Avg. no. of partners	Avg. duration	Avg. total cost	Avg. EC contribution
Phase I	11	14 months	€1.3m	€1.0m
Phase II	44	45 months	€43.0m	€28.2m

Source: CORDA data (Feb. 2015)

As of February 2015, all of the Phase I projects were completed, and a Phase II project in each focus area had begun, with just one Phase II project (SECUR-ED) completed, and another one (PERSEUS) soon to finish. The three remaining Phase II projects were still on-going (CORE, EDEN, DRIVER). Project details are presented below.

F.7.2 Phase I projects

Phase I – Project scope and objectives

The work programmes briefly outlined the scope and expected impact of Phase I demonstration projects, referring in particular to the required **strategic roadmap** and the need for **EU-wide awareness**:

- Scope: " The action will define the strategic roadmap required for the demonstration project which should take into account relevant completed, on-going and planned work and lay out, in a coherent and clear manner, the further research work required. It will assess the relevant factual and political situation and trends as well as potential classification requirements and issues related to IPR, also with a view to procurement. It will ensure EU wide dissemination of the preparation of the demonstration project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the cooperation of third country participants is required or recommended."
- Expected impact: "Through comprehensive preparation (not proposal preparation) of the demonstration project, the action will provide a solid basis for the description of its phase 2 in the Work Programme of Security Research Call 3 in 2009 as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified EU wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration project identifying key players and performance profiles of other required contributors, allowing for their effective and balanced access to the action. It will also achieve qualified EU wide awareness of relevant end users, governments and other bodies, facilitating and providing guidance concerning the real-life implementation of the system of systems to be demonstrated."

These specifications for Phase I projects were standard across all five demonstration areas.

Phase I – Projects and consortia

The following table presents the nine **Phase I demonstration projects**, organised according to relevant topics. The total cost for each project is also indicated.

Table 50: Distribution of Phase I projects by theme

Theme	Projects
Security of mass transportation	• DEMASST - Security of critical infrastructures related to mass transportation (€1.8m)
Integrated border control and management	• GLOBE - European Global Border Environment (€1.0m)
Logistic and supply chain security	• IMCOSEC - Integrated approach to IMprove the supply chain for COntainer transport and integrated SECurity simultaneously (€1.1m) • LOGSEC - Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security (€0.8m)
CBRNE	• DECOTESSC1 - DEmonstration of COunterTErrorism System-of-Systems against CBRNE phase 1 (€1.6m) • CBRNEMAP - Road-mapping study of CBRNE demonstrator (€1.7m)
Aftermath crisis management	• HELP - Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems (€1.4m) • CRYSIS - Critical Response in Security and Safety Emergencies (€0.8m) • ACRIMAS - Aftermath Crisis Management System-of-systems Demonstration (€1.7m)

Source: CORDA data (Feb. 2015)

Phase I demonstration projects involved 5 to 15 **partners** each (11 on average), with 103 participants in total across the 9 projects. Most were from private for profit organisations (excluding education) (PRC - 37%), or research organisations (REC - 37%), while the remainder represented higher or secondary education organisations (HES - 8%), public bodies (excluding research and education) (PUB - 5%) or other (OTH - 10%) organisations.

It is worth noting that three projects (DECOTESSC1, DEMASST and GLOBE) did not include end-users or industrial partners. However, all projects did employ certain **activities related to end-users**, even if they were not included as direct project partners. The means of involvement employed by the different projects included:

- Direct interviews with end-users (ACRIMAS);
- The organisation of workshops with end-users (DECOTESSC1);
- The setting up of expert groups (CRYSIS - User Advisory Board);
- The direct involvement of end-users in the consortium (ACRIMAS, CRISYS, HELP, IMCOSEC, LOGSEC, CBRNEMAP).

According to project leaders, the involvement of end-users was crucial to identifying needs and gaps, and also for validation purposes. Their inputs were also used to shape the final deliverables of these projects.

Phase I – Project activities, outputs and outcomes

Even though the thematic focus of the different Phase I projects varied, they had common **operational objectives and activities**. These were:

- To provide a **comprehensive definition of the system**, i.e. to draw boundaries for the scope of the demonstration phase;
- To provide **insight on the state-of-the-art** regarding all the solutions that could be used in the demonstration phase. This was mainly done by looking at outputs from completed FP7 projects and projects funded at national level, as well as existing standards and regulations, complemented by the knowledge of project partners;

- To **perform a gap analysis**, based on the state-of-the-art as well as on the expressed needs of various stakeholders (mainly academia, industry and end-users). This would also help to demonstrate the added-value of a European demonstration project. For example, the analysis of a projects on the security of critical infrastructure related to mass transportation (DEMASST) demonstrated the similarity of problems in different Member States;
- To **perform a gap analysis**, based on the state-of-the-art as well as on the expressed needs of various stakeholders (mainly academia, industry and end-users). This would also help to demonstrate the added-value of a European demonstration project. For example, project DEMASST: Security of critical infrastructures related to mass transportation, demonstrated the similarity of problems in different Member States;
- To **develop a roadmap for Phase II** projects to pave the way for Phase II calls for proposals.

These objectives led consortiums to look into various dimensions of security research issues: technical solutions, interoperability issues, legal basis, internal organisations, existing standards and so on. The subsequent outputs from Phase I projects took the form of symposia, orientation papers and roadmap documents.

According to those consulted, most of the Phase I projects were successful in fully **achieving their objectives**, i.e. identifying gaps, raising awareness among stakeholders and producing important inputs for the Phase II calls for proposals.

Participants believe that the projects built a common understanding of risks, gaps, target processes and suitable technologies and helped to clarify the notion of "system of systems", as they took into account different solutions and tried to make them fit into an integrated plan. They were also seen by those involved as a successful first step in the Demonstration phase of these projects. Indeed, a large proportion of participants in the Phase I activities went on to be part of the consortiums applying for the subsequent Phase II projects.

The positive effect of the Phase I projects contributed to shaping subsequent Phase II calls by providing greater detail, depth and focus to the requirements for the implementation phase of the demonstration programmes.

F.7.3 Phase II projects

Phase II – Scope and objectives

Following on from the nine initial projects, the Security Research Programme then sought to award a Phase II project in each of the five identified demonstration themes.

The basic expected **scope** and technical content of these projects had already been set out as part of the Phase I calls. For example, the 2007 Work Programme for mass transportation Phase I projects already indicated that the second phase would see:

> *"The demonstration of a consistent and integrated set of mass transportation security systems to secure transport networks, nodes and platforms, taking into account the specific requirements for each sector/mode and the particular cross-border dimension of mass transport."*

Drawing on the Phase I projects, the Work Programme parts related to full demonstration projects (issued from 2010 onwards) then elaborated and detailed the scope and purpose of intended Phase II demonstrations. For example, for urban public transport Phase II projects, the 2010 Work Programme details the **expected impact** as follows:

> *"The DP should provide a demonstration of "system of systems" solutions to enhance the security of urban public transportation for typical big and mid-sized European cities with over 0.5 million inhabitants. The challenge, the demonstrator has to tackle, is the security of mass transport in a metropolitan area and the proposed solution should be benchmarked according to their impact on improved security. The systems / technologies demonstrated should be demonstrated with 'real hardware' in a number of relevant places in addition to any modeling and simulation. The DP would nonetheless be required to have a fully European dimension, and make best use of the pertinent projects conducted within the*

national and /or European frameworks, focusing on their possible integration with a view to better responding to meeting operational challenges. The DP should make it possible to bring together private and public end users from many countries, able to provide the input data of the pertinent scenarios as well as the assessment (validation/test) criteria".

Similarly detailed explanations were given in the other four areas sought.

All five demonstration projects, while focused on very different themes and topics, had a central **common objective**, which was to integrate *existing* solutions into a 'system', in order to improve the capacity of EU stakeholders to respond to end-users' and citizens' needs regarding security and safety-related issues. Work Programmes for the Phase II demonstration projects also emphasised the need for an "integrated and scalable solution", and the need to provide guidance for adapting general solutions to local specificities.

Phase II - Projects and consortia

One **Phase II project** was selected for each of the five demonstration topics, as shown below. The general objectives of each project are also shown, to demonstrate the similarities in the overarching aims of these Phase II demonstration actions.

Table 51: Phase II projects by theme, and project objectives

Theme	Project title (total cost)	Project objectives
Security of mass transportation	SECUR-ED – Secured Urban Transportation: European Demonstration (€40.0m)	SECUR-ED will build a holistic and systematic all-risks approach to assess, prevent, detect, prepare for and manage the threats to mass transportation / urban and regional transport security is being sought.
Integrated border control and management	PERSEUS – Protection of European seas and borders through the intelligent use of surveillance (€43.6m)	The objective of PERSEUS is to build and demonstrate an EU maritime surveillance system integrating existing national and communitarian installations and enhancing them with innovative technologies.
Logistic and supply chain security	CORE – Consistently Optimised Resilient Secure Global Supply-Chains (€48.8m)	CORE will focus on consolidating solutions developed in completed projects and implement them in order to discover gaps and practical problems and to develop capabilities and solutions that could deliver sizable and sustainable progress in supply chain security across all EU Member States and on a global scale.
CBRNE	EDEN – End-user driven DEmo for CBRNE (€35.8m)	EDEN will provide solutions to improve CBRNE resilience and allow enhanced interoperability and effectiveness between CBRNE operators and ensuring the resilience capability of the EU society.
Aftermath crisis management	DRIVER – DRiving InnoVation in crisis management for European Resilience (€46.3m)	DRIVER will develop a distributed pan-European Test-bed enabling testing and iterative refinement of new crisis management solutions.

Source: CORDA data (Feb. 2015) and project websites

Phase II demonstration projects involved between 33 and 70 **partners** each (44 on average), with 218 participants in total across the five projects. Most were from private for profit organisations (excluding education) (PRC - 53%), or research organisations (REC - 20%), while the remainder represented public bodies (excluding research and education) (PUB - 12%), higher or secondary education organisations (HES - 9%), or other (OTH - 6%) organisation types.

A large number of Phase II project partners (especially those from academia and industry) were also involved in Phase I projects. For instance, eight of the 15 participants in the DEMASST Phase I project went on to participate in the SECUR-ED project, including as the coordinator.

The size of each Phase II consortium means that the budget for coordination activities was more significant than usual. It also led to project coordinators deploying specific project management arrangements, in order to manage the large-scale of the activities, and achieve the objectives of the projects. For instance, the SECUR-ED project was divided into five subprojects, with each having its own leader (from industry) and co-leader (from the end-user or research community).

End-users (consisting mainly of public administrations, first responders and final clients of the solutions being demonstrated) are playing a more **central role** than in many other FP7 Security Research projects. As well as participating through involvement in advisory groups, workshops, subscriptions to newsletters, etc. they are also part of the demonstration activities themselves, as direct participants. This is considered by project coordinators as the only way to make the project useful for end-users.

Moreover, in addition to the participation of individual end-users, several projects have included **end-user umbrella organisations** in their consortia: for instance, SECUR-ED involved the International Association of Public Transport (UITP), while CORE involved the World Customs Organisation, as well as the European Council of Transport Users as its coordinator. The involvement of these umbrella organisations is seen as an efficient way to reach a high number of end-users at the same time.

DRIVER is the only project that involves a standardisation body in the consortium, even though all projects have the objective to participate in the development of standards or common methods.

Phase II – Project activities, outputs and outcomes

The Phase II projects all build on previous project activity – both the Phase I demonstration activities, and other FP7 Security Research projects. For instance, the CORE project website[138] makes explicit that it is consolidating solutions developed through what it calls its "reference projects", which include CASSANDRA, CONTAIN, SUPPORT, SAFEPOST, EUROSKY and e-freight projects. This is helped by the fact that many of those involved in Phase II consortia, also had some involvement in at least one Phase I demonstration project.

Even though the five projects address very different issues, each is focused around three main phases of activities:

1. **A scoping and design phase**: The initial phase of each demonstration project relates to choosing the existing technologies and solutions to be integrated, determining how to integrate these solutions, and the construction of scenarios for demonstrating these. For some projects, these scenarios were already integrated into the project proposal (e.g. SECUR-ED, CORE). In some projects (e.g. EDEN), the first step was a consultation with end-users on their needs and expectations.
2. **Demonstration phases**: This is the core activity. The demonstration activities vary from one project to another. For example, the number of demonstration activities per project varies from two very large demonstrations (PERSEUS) to six smaller demonstration activities (CORE), while some combine practical forms of demonstration with simulation and virtual testing (DRIVER). The ambitions are also different: some projects' objectives are to provide end-users with a "plug-and-play" system, where different solutions and technologies can be added, with insights provided on the best solutions to choose based on their needs (DRIVER, SECUR-ED), while others sought to create a common system (PERSEUS) or to identify gaps and weaknesses in existing systems (CORE). However, in all cases, the core idea of the demonstration phase is to adapt existing technologies to make the system more efficient.
3. **A dissemination and improvement phase**: All projects include this phase of activity, although the details vary, with the type of demonstration activities influencing the subsequent dissemination actions. For example, EDEN planned to create a "toolbox of toolboxes", SECUR-ED a set of training guidelines, and DRIVER improvements to some of the existing solutions utilised by the project.

At the time of writing, only one of the Phase II projects (SECUR-ED) had finished, while another (PERSEUS) was close to completion. As such, the case focuses on these two examples to explore the **outputs and outcomes** of the demonstration projects.

[138] http://www.coreproject.eu/about.aspx

These two projects chose different strategies to demonstration: PERSEUS focused on experimenting with a European maritime surveillance system, while SECUR-ED tried to define a "plug-and-play" system, where different solutions and technologies could be added and adapted to different situations.

SECUR-ED demonstration activities took place in four cities (Madrid, Paris, Milan and Berlin), with each hosting several distinct scenarios. These demonstrations validated the security enhancement packages, and acted as showcases for the initiative. Further satellite demonstrations also took place in other cities, utilising the toolkit of solutions developed in the project. The project also actively disseminated results to the urban transport stakeholder community in Europe, even after the end of the project, including through participation in various conferences and contributions to standardisation. SECUR-ED's main reusable results were published in a White Paper for public transport stakeholders, which also detailed the main recommendations for implementers derived from the SECUR-ED experience.

The **PERSEUS** project has completed major demonstrations in 2013 (Portugal, Spain, France, Italy), 2014 (Greece) and 2015 (Canary Islands), as well as other validation tests in open waters. The project concluded with a final event at the end of June 2015. Ultimately, it is hoped that the strong collaboration between Member States within the multidisciplinary PERSEUS project team will help deliver comprehensive maritime surveillance from coastal regions to the high seas, and that in the future, these systems could be used within a network to continuously monitor maritime areas of interest.

According to stakeholders, both projects have been successful. In particular, both managed to **integrate targeted stakeholders** within the project, including various end-users. For SECURE-ED this included industrial partners, transport organisations and public security forces, while for PERSEUS this included European agencies, border control authorities and industrial partners. Both were also able to use demonstration activities to **validate** the use of a "system of technologies" in real-life conditions, showing the possibilities to innovate and to improve actual systems. Finally, both have led to the production of a series of outputs, including **guidelines** on how to replicate or use the results of the projects.

F.7.4 Issues and limitations

Although the **Phase I projects** are generally considered to have met their objectives, their deployment has not been without issue. In particular:

- Phase I projects were supposed to provide a comprehensive view of the existing solutions in one domain. However, the short **duration of these projects** is felt to have allowed insufficient time for such a thorough state-of-the-art analysis to take place. The short timescale also created issues with the projects being able to properly engage the end-user community.
- Because most Phase I projects were conducted early in the FP7 Security Research Programme, they could not benefit fully from the outputs of many FP7-funded capacity and integrated projects. Given the 'umbrella' role of the demonstration building block within the framework of the Research Programme as a whole, and the specific requirements on Phase I projects to take account of existing knowledge and activities, this **timing issue** is seen as a potential weakness.
- For some topics, several Phase I projects were selected. Even though these projects did not have the exact same focus, stakeholders suggested that **overlapping (duplicative) research activities** took place between, and there was no obligation on these projects to cooperate or coordinate to ensure that this did not happen. It was also suggested that the multiple, and sometimes overlapping, Phase I projects may have made the process of shaping calls for Phase II projects more complicated.

However, it should be noted that longer Phase I projects, or their delayed deployment, would not have allowed sufficient time to then propose and undertake Phase II demonstration projects within the seven-year period of FP7.

Similarly, stakeholders involved in the demonstration projects have also pointed to a small number of issues that may limit the success of the **Phase II activities**.

The Demonstration projects have ambitions relating to EU-wide systems. However, the **fragmentation** of the end-users' landscape in the EU as well as legal issues can be barriers to the adoption of pan-European solutions. This fragmentation is one of the issues that the demonstration projects sought to address, or at least take into account, through their activities. However, stakeholders suggested that more focus and effort might be needed in relation to the barriers to adoption of the demonstrated solutions by different actors across different countries.

The involvement of end-users in demonstration projects is seen as crucial, as it is a way to ensure that the solutions that are demonstrated are in line with their needs. However, participating end-users (who have generally been well engaged in the demonstration activities) are not often the actual **buyers of solutions** (often national ministries). The lack of engagement with the 'buyers' may limit the likelihood that (or speed with which) solutions are adopted after the projects. However, the involvement of government ministries in projects is often based on a political decision that is hard for the Research Programme to influence. One example where such bodies have been heavily involved is CORE, which included several national customs authorities and relevant national ministries, as well as the World Customs Organisation and Interpol in its consortium.

Overall, demonstration projects are seen as a means to develop integrated solutions and reduce market fragmentation in the EU. However, demonstrating that a solution is useful and efficient is not enough on its own to make it a commercial success. This is something that the stakeholders consulted feel should be tackled at an early stage in planning of demonstration projects.

F.7.5 Conclusions and lessons learnt

Phase I projects are felt to have been successful in paving the way for large-scale demonstration activities within the FP7 Security Research theme, even though the time frame for these projects limited the ability of partners to integrate all the emerging and existing solutions on one topic. The roadmaps produced in these projects were used as a major input for the Phase II calls for proposals, and a large number of participants to these projects also went on to be part of consortiums for Phase II projects.

As most demonstration activities were not complete at the time of writing, few conclusions can be drawn regarding **Phase II projects**. However, feedback on the first two projects suggests that these have been successful in experimenting with the integration of different solutions in "real-life situations", thanks to significant commitment from core management teams (and a significant budget dedicated to coordination), as well as strong involvement of end-users.

It will take more time to measure the impacts of these projects. However, there are already concerns that the fragmented EU end-user landscape, and the separation between end-users and solution-buyers may prove to be barriers to prompt and widespread adoption of demonstrated solutions.

Several other lessons might be drawn from the analysis and interviews.

In relation to the **participation of end-users**: As for other security research projects, end-user involvement in demonstration projects can be difficult, especially because these organisations are often not used to being part of R&D projects. It is however possible to make the most out of their participations, through very early involvement in the definition phase of projects (Phase I and early Phase II), as well as through direct or indirect communication. This can be done through end-user coordination (CORE), the participation of an umbrella organisation (SECUR-ED), or through workshops (DRIVER: interoperability workshop). It also seems that an efficient way to increase awareness around a project is to set up communities of interests (e.g. DRIVER). This might be easier when communities are well defined and rather small (CBRNE). In such cases, umbrella organisations can play an important role as intermediaries (CORE or SECUR-ED). In order to increase the potential impacts of projects and the usefulness of outputs for end-users, it is also important to clarify whether or not end-users are also potential clients / buyers for the solution. If not, partners should push for the integration of final clients in the consortium as well.

In relation to the **legal framework and national specificities**: Non-technical issues are important for such projects, as they deal with very broad policy areas, with complex legal basis – especially when they focus on cross-border issues such as PERSEUS – and strong national interests and specificities. This has to be taken into account in the text of the Work Programme, as well as in both phases of project, in order to ensure solutions are both useful and relevant. This could also mean that the scope of such Demonstration projects should be adapted to the feasibility and the state-of-play regarding legal issues.

In relation to the **scale and scope of projects**: Each demonstration project focuses on very different areas, with different cultural, legal, ethical and technological issues. This should be taken into account when drafting Work Programmes: for example, with some demonstration projects being very large and focusing on developing EU-wide solutions, while other areas call for more modest demonstration activities and goals (e.g. where "system of systems" solutions are not yet appropriate).

F.8 Protecting critical infrastructures – Port Security

The objective of **this case study** is to explore how port security was addressed through the FP7 Security Research Actions – both at a programme level, and through individual projects that have wholly or partially tackled the issue. It considers the activities and results of these projects, and draws conclusions and lessons for the future. The case study contributes to the evaluation of the Programme's effectiveness in improving security capabilities and reducing gaps.

The case study will proceed in the following way: First, the introduction outlines the issues of port security and the scope of the study. Second, the position of port security within the FP7 Security Research programme is described. The subsequent three sections examine FP7 Security Research projects that address port security issues before turning to end-user involvement in these projects. Finally, conclusions and lessons are drawn from the case study.

The research carried out in the preparation of the case study consisted of analysis of programme data from CORDA and interviews with four experts from the European Commission, research organisations and private companies.

F.8.1 Introduction

A **port** is a specified area of land and water, containing works and equipment designed to facilitate commercial maritime transport operations[139]. It is a rather complex entity that serves **three main functions**:

- Movement of freight across the interface from sea to land and vice-versa, whereas the freight can take man different forms ranging from containers over liquids to bulk materials;
- Movement of passengers arriving and leaving by ship, car and/or train; and
- Servicing of maritime vessels, e.g. offering supplies, maintenance, waste management.

In addition, many ports also provide **two secondary functions**, as they

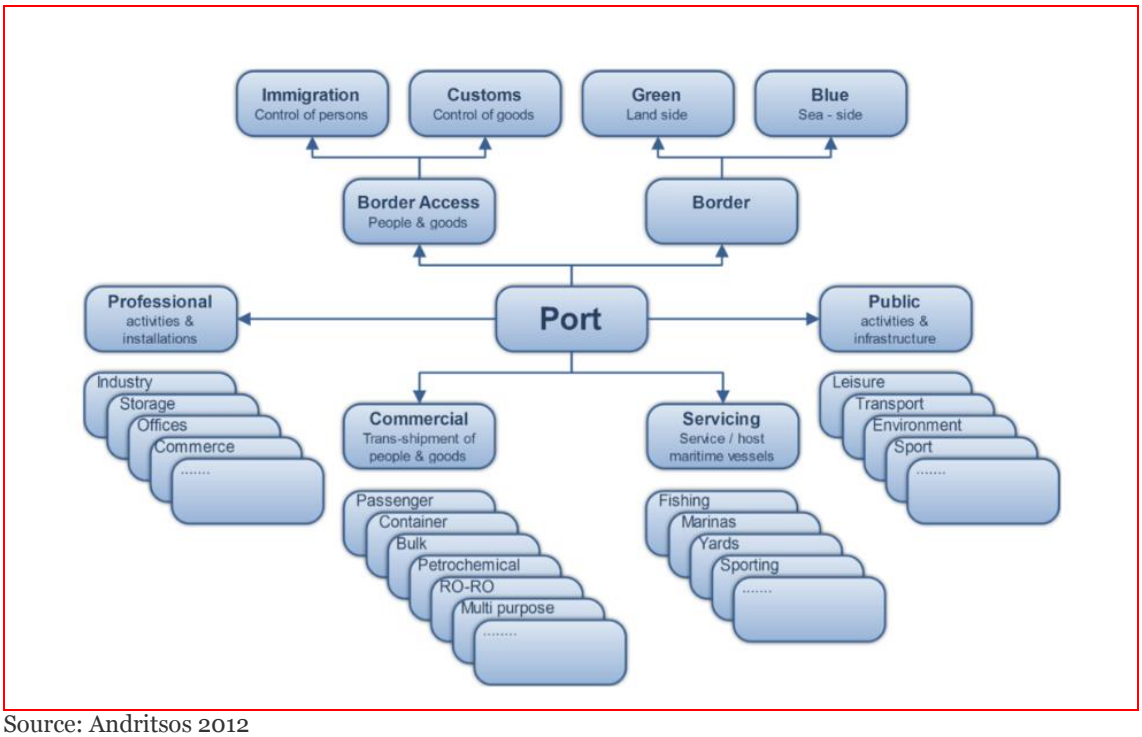
- often serve as borders, for people and freight to be admitted and controlled, i.e. they are points of control for customs and immigration agencies;
- provide professional and public functions to the region or community in which they are situated (Andritsos 2012)[140];
- While the former are concerned with structures and activities of industry, commerce, storage, logistics etc, the latter include structures and activities such as leisure, transport, environment, sports, or tourism.

[139] Directive 2005/65/EC.

[140] Andritsos, F. (2012) EU Port Security and Growth, European Commission – Joint Research Centre, Conference Paper presented at the 8th Future Security Conference, Berlin 2012.

Figure 28 illustrates these different functions of ports and underlines the complexity of interactions, as well as the multitude of actors required to operate them and interacting in them.

Figure 28: The multiple functions of ports



Source: Andritsos 2012

To provide these functions ports require structures or installations, so-called **port facilities**. They include, for examples terminals for containers, cruise ships, ferries, liquid bulk materials such as petrochemicals, for gas or for dry bulk. The term may also refer to terminal buildings, delivery areas, security systems, control centres and goods storage areas, parking lots and railway installations in the ports, as well as anchorages, awaiting berths and approaches for ships from the sea[141].

Port security is concerned with the safe operation of port facilities, which gives rise to a number of specific challenges, as ports:

- Are **important nodes** in freight and passenger transportation, given the sheer number of passengers they serve and the amount of goods they process, which both imply a significant economic importance of ports[142];
- Are close to often densely populated areas with their own infrastructures, industrial installations, cultural heritage and natural sanctuaries;
- Cover **large areas of land and sea**, a fact that implies challenges of clear demarcation, access control and surveillance, ports involve sophisticated operational infrastructures of land, rail and sea logistics that need to interact smoothly and often in a just-on-time manner to ensure most efficient services; and
- Are points where security is provided by a **variety of public and private actors** such as port operators, private security firms, customs, border control authorities, the police and

[141] Regulation (EC) No 725/2004.

[142] More than 90% of Europe's external and 40% of its internal trade is seaborne, while 3.7 billion tonnes (2012) of freight are loaded and unloaded and some 398 million passengers pass through EU ports each year. Europe's energy security also largely depends on shipping and the related infrastructures. Ensuring the effective functioning and the security of ports is therefore essential for the economic wellbeing of the EU. See http://cordis.europa.eu/result/rcn/158115_en.html.

border control. These authorities operate according to different rationales and on the basis of their own legacy systems, which are not always interoperable.

Over the past two decades, the issue of **port security has become increasingly important**. While security was not a major consideration for port development prior to the terrorist attacks of 11th September 2001, new security concerns have led to tighter border controls and increased vigilance (e.g. in the inspection of import cargos), and consequent higher costs for shippers and consumers. EU measures are often the result of adapting to international obligations of Member States, which negotiate new rules at international forums such as the International Maritime Organisation (IMO). Based on the international agreements the EU then implements European-wide minimum security standards.[143]

In response to the attacks of 9/11, and out of a growing concern for the security of ships and ports, the **IMO drew up new security regulations**. These were implemented in a new chapter of the International Convention for the Safety of Life at Sea (SOLAS) and in the International Ship and Port facility Security (ISPS) code on minimum security arrangements for ships and port facilities.

The ISPS focuses under the notion of "maritime security" on the security of ships and port facilities. It has been introduced into **EU legislation** since 2004[144] and extended to cover the entire port area. The legislation requires that every port facility have a Port Facility Security Officer and a Port Facility Security Plan. The latter is formulated after a Port Facility Security Assessment, which is to be carried out by a governmental body or by specifically designated security organisations. The plan has to be approved by the authorities, reviewed and updated periodically (Andritsos 2012).

The European Commission[145] identified ports also as key transport infrastructures and one of several **critical infrastructures** in Europe. Critical infrastructures are defined as physical and virtual facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens, or on the effective functioning of governments in EU countries.

Already at this point it becomes clear that the issue of port security touches upon a number of security areas. It is likely to be addressed in a **variety of ways** or – more precisely – under a variety of "headings", for example "infrastructure", "maritime security" or "transport security" (Argomaniz 2011). It can be expected that security research will tackle issues of port security in a similarly diverse manner.

What are the **specific security challenges** that ports face? Three types of issues seem to be of particular importance:

- "Physical access control: control of the flow of persons, typically through perimeter security and access control measures;
- Material items flow control: screening of cargo, luggage, personal items, equipment, consumables etc.;
- Information flow control: efficient and secure management of information concerning the movement of vessels, vehicles and goods; communications"[146].

All three challenges and in particular the latter one, call for **interoperability**. Interoperability refers to the ability of systems to collaborate at the levels of information exchange, communication, operational procedures including training, organisational/business models and legal requirements, i.e. interoperability refers to technological, organisational and legal aspects. In the case of port security it is implied that it works across different organisations and different

[143] Argomaniz, J. (2011) The EU and Counter-Terrorism. Politics, Polity and Policies after 9/11, Routledge Abingdon.

[144] Regulation 725/2004 and Directive 2005/65/EC.

[145] COM(2004) 702.

[146] Andritsos, F. (2012) EU Port Security and Growth, European Commission – Joint Research Centre, Conference Paper presented at the 8th Future Security Conference, Berlin 2012.

types of handled materials, as well as security issues. The individual requirements are "highly case specific" (Andritsos 2012).

The need to ensure interoperability – with existing systems as much as with newly developed solutions – also stems from the fact that ports operate in a competitive environment. Security is often considered as an add-on **cost** that weakens the competitive position. Only an integrated and systemic approach that makes full use of the available data and information across the board of all organisations involved, is likely to be accepted and supported by all parties involved. Consequently, the integration of different systems and even of systems of systems is likely to be of particular importance for security research.

F.8.2 Port security within the FP7 security research programme

The European Security Research Advisory Board's (**ESRAB**) 2006 report[147] identified port security as an area of strategic interest for security research, and one which fell within the scope of two of the four security missions of high political relevance, namely 'Border Security' and 'Critical Infrastructure Protection'.

Consequently, the Preparatory Action for Security Research (**PASR**) picked up on the topic. From 2004 to 2006 the PASR supported actions for improving "situation awareness". The latter referred to "threats that could affect Europe, particularly land and sea borders and assets of global interest"[148], which includes port facilities. The gathering, analysis and appropriate integration and dissemination of information about land and sea borders were considered to be the key ways to address the threat. To this end, specific capabilities i.e. concepts and technologies – as opposed, for example, to integrated systems of components – were to be developed and demonstrated. Port security was treated here as part of border surveillance.

Similarly, in the first Work Programme (2007) of the FP7 Security Research programme port security was explicitly targeted, within the 'intelligent surveillance and enhancing border security' mission area. The topic – '**Main port area security system** (including containers)' – aimed to improve situational awareness at key ports through the monitoring and tracking of complex port environments. It called for the creation of an integrated port area security system, capable of providing accurate situational awareness and of alerting security operators to required interventions. The call attracted only a small number of proposals, and these were not judged to have adequately met the expectations of the call. As a result, no projects were selected.

The call was reissued in the second Work Programme (2009), again under 'Intelligent surveillance and enhancing border security'. It was slightly amended and came with a more elaborate explanation of the topic. This time, the call resulted in the award of project **SUPPORT**. SUPPORT (discussed in more detail further below) sought to address port security with a comprehensive approach that accounted for the complexity and diversity of ports and build on the integration of legacy port systems for surveillance and information management.

The subsequent Work Programmes in 2010 and 2011 the Commission continued with a call for integration projects and added **demonstration programmes** to the portfolio. The 2010 Work Programme included topics on European-wide integrated maritime border control systems, and the monitoring and tracking of shipping containers, both of which included elements of port security; while the 2011 annual Work Programme included a topic on 'border crossing points of the future', which included ports as one form of border crossing.

The demonstration project funded under the 2010 call is **PERSEUS** ("Protection of European seas and borders through the intelligent use of surveillance"). PERSEUS addresses challenges like complex security mission including migration and trafficking, with the overall objective to deliver tested, demonstrated and validated recommendations for the European wide integrated maritime border control system, in line with the EUROSUR objectives"[149]. All in all 32 partners from 12 countries, including many public authorities such as the Guardia Civil (Spain) or the

[147] European Security Research Advisory Board (2006) Meeting the challenge: the European Security Research Agenda.

[148] Commission Decision C(2005)259.

[149] http://cordis.europa.eu/project/rcn/97515_en.html

Ministry of Citizens Protection (Greece) as well as NATO Undersea Research Centre, participate in the project.

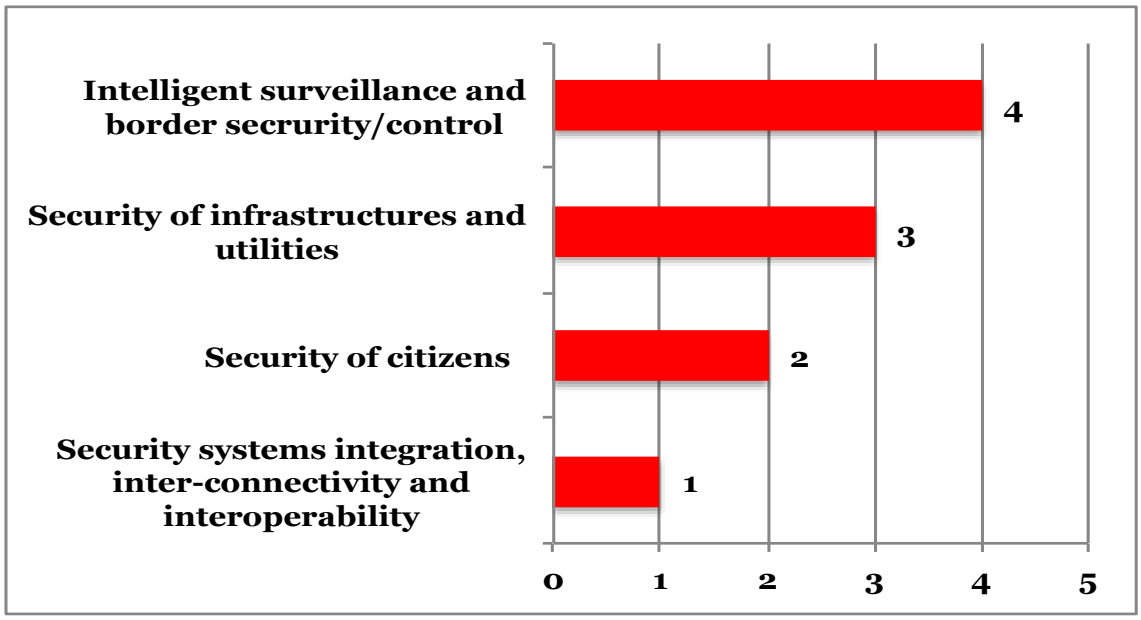
As the political and strategic agenda started putting an increasing emphasis on issues such as illegal immigration, as opposed to large-scale terrorist attacks, issues of port security was **subsumed under other headings**, in particular as part of maritime or transport security. As such, no explicit mention of ports or port security was made in the 2012 and 2013 Work Programmes, other than in relation to a call for projects that should develop a research agenda for future security research on land transport (with ports being one form of transport hub), and a call for projects that would test the interoperability of maritime surveillance systems. This does not mean that port security is not researched anymore under the Security Research Actions but rather that it has become part of a wider, more comprehensive security research agenda.

F.8.3 FP7 Security projects addressing port security

Within the FP7 Security project portfolio, **eleven projects** have been identified that address port security issues to some degree (determined by the mentioning of "port" in the project abstract). As one might expect, given the assessment of the Work Programmes above, most of the eleven projects originated in the earlier part of the Security programme. Specifically, four projects resulted from the 2007 calls, three from the 2009 calls, and then one from each of the three subsequent calls (2010, 2012 and 2013). While eight of these projects have been finalised, two are still on going.

The figure below shows the distribution of projects across the areas of the programme. Nine of the projects fall within three of the four main **mission areas**, while the final project is located in the cross-cutting area of 'security systems integration, inter-connectivity and interoperability'. Unsurprisingly, the majority of the projects fall within the two mission areas that align with the security missions identified by ESRAB (i.e. 'Border Security' and 'Critical Infrastructure Protection').

Figure 29: Distribution of projects with a "port security" dimension by mission



Source: Technopolis analysis of CORDA data, January 2015

These projects with a 'port security dimension' involved over 307 participations and 243 unique organisations (participants) between them. Five of the projects benefited from the direct participation of at least one port authority (i.e. a key end-user of port security research). These projects are listed below, with the relevant port authorities.

Table 52: List of projects with the participation of port authority bodies[150]

Mission	Project acronym	End-user organisation involved
Smart surveillance and border security	SUPPORT	Port of Lisbon Administration, Portugal
		Piraeus Port Authority, Greece
	EFFISEC	Port of Lisbon Administration, Portugal
	CONTAIN	Port Authority of Valencia, Spain
Security of citizens	UNCOSS	Dubrovnik Port Authority, Croatia
		The Port of Bar Holding Company, Montenegro
Security of infrastructures and utilities	SECTRONIC	La Spezia Port Authority, Italy

Source: Technopolis analysis of CORDA data, January 2015

Only one of the projects – SUPPORT – was exclusively focused on the issue of port security. The other projects were not specifically and solely dedicated to port security issues; they included components relating to port security, but only as part of a broader set of issues being tackled.

F.8.4 The SUPPORT project

The **SUPPORT project – Security UPgrade for PORTs**[151] – recognised the importance of port security for Europe, both in terms of threats to human life and the economic damage that could arise from attacks on port facilities. It also recognised the challenges faced in improving port security, due to their complex operational modalities and the lack of efficient organisational and technological interfaces between the different agencies and operators concerned. The project therefore sought to address 'total' port security solutions – encompassing legal, organisational, technological, training and human aspects – that would also integrate legacy port systems with new surveillance and information management systems.

The project brought **together 22 partners from 13 European countries** in an effort to create innovative, versatile, configurable and highly automated port security solutions that could operate in complex port environments, and bring about a new generation of port security practices. The majority of these partners were from the private sector, and included a number of port authorities and their clients, who are the end-users of security systems, and who were selected to represent typical, but different, port-related operations across Europe.

The project aimed to engage these representative stakeholders in the **development of next generation solutions** for preventative and remedial security capabilities. The project built on achievements in port security (e.g. the ISPS code) and brought together advances from security research with the results of EU projects in maritime and intermodal transport. It also adopted a stakeholder approach, firmly grounded on the perspective of the end-users. In particular it built on the experience of consortium members with responsibilities in ports and the supply chain (e.g. port authorities, port and transport operators and governmental organisations). Starting from the perspective of these partners' port operations, the project was able to identify major security gaps, and produce generic port security models that describe security measures to maintain or increase the level of efficiency and safety of these ports. These models were intended to be sufficiently adaptable to suit different configurations of ports depending on their specific security gaps.

The key output from the project was the **Port Security Management System** (PSMS), which was designed to help Port Facility Security Officers (PFSOs) upgrade their security systems by empowering them with knowledge. It includes five elements:

- A maturity module, designed to enable security professionals to review and upgrade security plans and address terrorist threats
- A corporate security module, which addresses crime risks, such as loss events, related to corporate processes and procedures

[150] Port of Lisbon Administration was also part of the EFFISEC project, which does, however, not focus on port security, an aspect that is also reflected by the fact that its abstract does not make reference to the topic of port security.

[151] http://cordis.europa.eu/project/rcn/94831_en.html

- An e-learning education and examination module based on best practices of ISPS-related maritime security education including drills and exercises
- A sharing and decision support module, which enables security professionals to supervise facilities via the internet and collaborate on local, national or global scale
- An Authorised Economic Operator (AEO) security self-assessment module, which provides a system to reach compliancy and submit AEO applications

The PSMS provides information, skills and methodologies that enable the PFSOs to maintain, evaluate and upgrade their security measures and create security awareness without major investment. The system also delivers outputs in the form of graphics that can be used to reinforce messages about security threats and mitigation measures.

As part of the project, **full-scale demonstrations** were organised in EU ports (Gothenburg, Lisbon and Piraeus) and augmented with a broader evaluation programme by members of a security forum for European ports. The Port of Dublin (which was not a partner in the project) has already bought this technology.

F.8.5 Other port-related projects

The **ten other port security-related projects** within the portfolio that have been identified as addressing one or more components of port security are listed below.

Table 53: Distribution of projects by mission

Mission	Project acronym	Full name
Smart surveillance and border security /control	CONTAIN	Container Security Advanced Information Networking
	EFFISEC	EFFicient Integrated SECurity Checkpoints
	FASTPASS	A harmonised, modular reference system for all European automatic border crossing points
	SEABILLA	Sea Border Surveillance
Security of infrastructures and utilities	SECTRONIC	Security System for Maritime Infrastructures, Ports and Coastal Zones
	ADABTS	Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces
	CORE	Consistently Optimised REsilient secure global supply chains
Security of citizens	IMCOSEC	Integrated approach to improve the supply chain for container transport and integrated security simultaneously
	UNCOSS	UNderwater Coastal Sea Surveillance
Security systems integration, inter-connectivity and interoperability	STAR-TRANS:	Strategic Risk Assessment and Contingency Planning in Interconnected Transport Networks

Source: Technopolis analysis of CORDA data, January 2015

These projects do not only address port security, but rather they **include a port security-related component** within a wider set of activities. For example, issued addressed by the projects include:

- The improvement of maritime surveillance systems. **SEABILLA** (Sea border surveillance) aimed at creating an architecture for cost-effective sea border surveillance systems at the European level.
- The surveillance and protection of critical maritime infrastructures, ports and coastal zones. The **SECTRONIC** project scope covered ports, cruise vessels, energy production and transport. It aimed at creating a system that could help protect ports, ships and energy infrastructure from being damaged by deliberate acts of terrorism, human negligence, accidents or criminal activities.
- Smart containers. The **CONTAIN** project aimed at specifying and demonstrating a European Surveillance system for Shipping Containers. The latter was supposed to enable ports to establish upgraded security processes for port containers, and provide information feeds to port community systems.

Many of these projects have led to the **development of improved technologies**. For instance, the UNCOSS project, which aimed to develop detection systems to identify weapons

sitting on the seabed, succeeded in providing a fundamental technology for the global issue of maritime surveillance and ports / naval infrastructure protection, with the production of a prototype of a complete coastal survey system.

Other projects led to **field demonstrations of proofs of concept** and prototypes. For instance, the SECTRONIC project resulted in field trials of 13 security scenarios, with sensors and communication equipment assessed through field evaluation against real targets. The SECTRONIC system was then developed and installed in ports (Rotterdam and La Spezia) during a one-year operational evaluation period, and is considered to have performed well.

F.8.6 End-user involvement

It is worth highlighting that not only the main project addressing port security (SUPPORT) but also a number of projects including port security-related components within a wider set of activities have made real efforts to actively **involve end-users**, who have been able to provide the projects with a better understanding of user needs, and practical realities.

- In this regard, the **SUPPORT** project is particularly interesting in that it involved end-users from the very beginning of the project, i.e. at the stage of the technical design. This project also included training for participating port staff, as well as dissemination activities for other ports and other possible stakeholders.
- The **SECTRONIC** project was also an end-user driven R&D project, characterised by close cooperation between R&D partners and end-users throughout. It resulted in field trials involving end-users representing the major market player in each of the three infrastructures addressed by this project (passenger transport, energy production/transport, commercial ports and combined military/commercial ports).
- End-users have also been involved into the **SEABILLA** project from the very beginning. Indeed, the project was based on requirements for Sea Border Surveillance defined by experienced operational users, through end-user workshops.
- In the **UNCOSS** project, partners included three ports of Croatia and Montenegro, who were heavily involved in the project, organising various meetings and workshops.

On the whole, end-users are considered by those consulted for the purpose of this case study to have played a helpful role in guiding the technological developments of projects. Their input was considered as extremely valuable, particularly in achieving more user-friendly outputs.

F.8.7 Conclusions and lessons learnt

Ports are of particular importance for Europe's economic prosperity, as more than 90% of Europe's external and 40% of its internal trade is transported by sea. Modern ports face **multiple challenges** and a far wider **range of threats** than has been the case historically, requiring comprehensive and reliable security solutions. Moreover, ports are nodes where highly complex systems of freight and passenger transportation interact and where a multitude of private but also public actors need to collaborate closely to ensure a smooth functioning of processes. Both aspects call for a systematic approach to security that ensures interoperability between systems and across all actors.

The FP7 Security Research Actions have addressed the specific requirements of port security through the different 'research routes'. Next to developing capabilities for port security, the SRA have in particular focused on **integration projects,** as well as a demonstration programme in the area of maritime security and border control that have also addressed issues of port security.

While only one project, **SUPPORT**, was exclusively focused on the issue of port security, in total **eleven projects** have been identified that address port security issues to some degree.[152]

It appears from the projects studied here that the **demand-based R&D** approach is beneficial, and can increase the impact and effectiveness of EU funding. It can also shorten time to market,

[152] The case study took those projects into consideration that mention "port" security in their project abstracts.

because R&D is in line with end-users needs from the beginning, and because the participation of industrial companies ensures that results can be marketed soon after the end of the project.

End-users, in particular public authorities, have played a key role in port security projects. They have assisted researchers in identifying gaps and vulnerabilities in protection systems. Their involvement in the development process is seen as a crucial, specifically:

- During the testing phase;
- When matching the technology to operational realities;
- When defining the application parameters; and
- In understanding the implementation process.

End-users often played a significant role during project **design and implementation** in the field of critical infrastructure protection. Such projects have had a strong, practical aspect in that they offered solutions directly applicable to already existing infrastructures. End-users quickly identified what works well or not, and provided guidance to project coordinators.

In addition, the involvement of end-users also helped to ensure the **application** of research results. Moreover, **testing** a security system developed through a research project on end-users' infrastructures is seen by those interviewed for the purpose of this case study as a good practice to be expanded. The projects reviewed in this case study seem to prove that an active integration of end-users is possible, particularly in the case of demand-driven and market-oriented R&D projects.

The case has shown that the active involvement of end-users has been a hallmark of the port security projects funded under the FP7 Security Research Actions. Their active involvement should be **maintained and broadened for the future**. Moreover, the Commission should explore ways to build on the experience of these projects with regard to end-user involvement and to transfer the lessons learned to other (mission) areas, where end-user involvement has remained a challenge.

In this context there is a need to bring the different actors, in particular **public actors**, involved in the provision of port (and maritime) security closer together. This is a challenge, given that the responsibility for different port security aspects is often spread among different actors at national level. However, they need to cooperate closely, to provide security, not least through the exchange of sensitive information. The project C*ommon Information Sharing Environment* (EUCISE)[153] addresses this issue, among others, for the area of maritime surveillance. Similar initiatives seem to be in order to build the trust among public authorities involved in port security that is necessary to share sensitive data and experience.

Finally, **interoperability** through systems integration – and this concerns not only technical but in particular organisational and legal systems – has been a challenge addressed by several research projects addressing also port security issues. Again, the Commission should investigate possibilities to distil the experience made by projects and to transfer the lessons to other mission areas.

[153] For more detailed information see http://www.eucise2020.eu/.

F.9 Tools, methods and resources to restore safety and security in case of crisis

This case study explores a selection of FP7 Security Research Programme projects dedicated to the development of EU common methods, tools and resources to restore safety and security in the case of crisis. It reviews the activities and outputs of these projects, and assesses the extent to which they have successfully contributed to more effective cooperation between Member States in the event of cross-border crises.

To focus the case, the scope has been limited to a number of projects funded through the 'restoring security and safety in case of crisis' mission area of the Security Research programme. However, it is recognised that there are more relevant projects (i.e. that involve developing common EU methods, tools and resources), which were funded in other programme areas – and particularly the cross-cutting domains of 'improving security systems integration, interconnectivity and interoperability' and 'security and society'.

The research conducted in the development of the case included document analysis, semi-structured interviews with five experts (from the European Commission and four organisations involved in relevant research projects) and the analysis of statistical data collected in the CORDA database.

F.9.1 Introduction

Cross-border crises within the EU often call for the cooperation and coordination of efforts of several Member States.

In its 2006 report, the European Security Research Advisory Board (ESRAB) acknowledged the **evolution of crises in recent decades**, and the shift towards increasingly "unpredictable catastrophic events"[154]. These developments, the Board stated, created a need for **new and innovative solutions** (tools, infrastructures, procedures, resources) that would allow for cooperation between Member States in crisis and emergency management, as well as more efficient and effective response and recovery, both during and after an incident.

Already the 2010 EU Internal Security Strategy reaffirmed these findings[155]. It identified increasing Europe's resilience to crises and disasters as a strategic goal for the EU's internal security policies, and highlighted the challenge faced in improving cooperation between Member States. Specifically in relation to R&D, the strategy highlighted that "interoperability of different technology systems used by any agency or service must be a strategic objective so that equipment does not pose a barrier to cooperation between Member States on the sharing of information or the carrying out of joint operations".

Taking account of the recommendations of ESRAB, 'Restoring security and safety in case of crisis' became one of the four **thematic missions** of the newly established FP7 Security Research Programme, and it is this area that is the focus of the case.

The first (2007) Work Programme explained that the 'restoring security and safety in case of crisis' activity area would address **two main challenges**.

- The first challenge was to ensure that governments, first responders and societies are better prepared *prior* to unpredictable catastrophic incidents, using new, innovative and affordable solutions.
- The second challenge was to improve the tools, infrastructures, procedures and organisational frameworks to respond and recover more efficiently and effectively both *during* and *after* an incident. The particular types of crisis to be addressed in both cases would cover: terrorist attacks and organised crime; natural disasters and pandemics; and major industrial accidents or technological disasters.

From 2011, the activity area was reorganised into four main areas: preparedness, prevention, mitigation and planning; response; recover; and CBRN response.

[154] European Security Research Advisory Board (2006) Meeting the challenge: the European Security Research Agenda.

[155] European Union (2010) Internal security strategy for the European Union – Towards a European security model.

F.9.2 Selected projects

As of December 2014, 55 projects had been funded through the 'restoring security and safety in case of crisis' mission area of the FP7 Security Research Programme. From a reading of the project abstracts, it would appear that at least 42 of these projects dedicated at least some of their resources to the development of methods, tools and resources that could be used in case of emergency.

The majority of these 42 projects are collaborative projects, but there are also a small number of coordination and support actions in the portfolio. The average project size within the selection is smaller than the overall Security Research programme average, with an EC contribution of €830k per project, compared with €4.1m per project overall. Within the selection, Higher or Secondary Education (HES) and Research Organisations (REC) represent around 40% of participants, and Private-for-Profit Organisations (excluding education, PRC) around 44%, which broadly aligns with the entire programme.

Among the selection of projects, it is possible to find three main clusters:

- Projects with a clear focus on **developing a common EU solution** – including Phase II demonstration projects
- Projects with a clear focus on developing a **specific tool / method,** with the intention of **fostering greater interoperability / cooperation**
- Projects with a focus on a **specific tool/ method,** and which **include activities related to their cooperative use** (mostly in the dissemination work package)

Most of the projects in the selection address interoperability and cooperation between different EU actors involved in crisis management (i.e. improving working across organisational boundaries). Only a small number explicitly set out (within their project abstracts) to address or support cross-border cooperation (i.e. improving working across national boundaries). Examples of the latter include (with relevant extracts taken from project abstracts):

- The **FAST-ID**[156] project, which sought to develop an information management and decision support system for improved disaster victim identification, which would "be used worldwide", "incorporate full consideration of different national considerations", "support information sharing and cooperative planning across organisations and nations", and ultimately "optimise international cooperation"
- The **INDIGO**[157] project, which would "propose a European emergency symbology reference for 2D/3D maps", offering a "visual reference to be used across Europe".
- The **ACRIMAS**[158] project, which sought to develop a roadmap as the basis for a phase II demonstration project, which would ultimately facilitate "European wide collaboration, cooperation and communication in crisis management".
- The **EULER**[159] project, which aimed to demonstrate how the benefits of Software Defined Radio could be leveraged to "drastically enhance interoperability" in case of crisis, and to "shape a European vision for interoperability in joint operations".
- The **IDIRA**[160] project, which sought to develop a system of technologies and guidelines which would help in "optimal resource planning and operations across national and organisational borders" in relation to disaster management.
- The **PRACTICE**[161] project, which aimed to create a concept and system that would "provide the EU and member states with a flexible and integrated system for coordinated response to

156 http://cordis.europa.eu/project/rcn/94293_en.html

157 http://indigo.diginext.fr/EN/index.html

158 http://cordis.europa.eu/project/rcn/98966_en.html

159 http://cordis.europa.eu/project/rcn/95202_en.html

160 http://cordis.europa.eu/project/rcn/98968_en.html

CBRN terrorist attack, which is easier to adapt to various national organizations and regulations".

- The **FORTRESS**[162] project, which sought to develop an Incident Evolution Tool (FIET), "with cross-border capabilities that can be used in a cascading crisis".
- The **TACTIC**[163] project, which aimed to develop a preparedness audit that would enable communities to assess impacts and prepare for "cross-border disasters".

Most of the projects in the selection address tools and methods that can be used in all types of crisis, but some are more specific (e.g. tools and methods in response to fire or a CBRNE attack). Between them the projects also address a range of crisis operations and functions, including: doctrine and operations; command and control, information management and communication; incident response, intervention and neutralisation and detection, identification and authentication, positioning and localisation.

The projects have different ambitions in terms of the tools and methods they set out to design and develop:

- Several focus on the development of online platforms (i.e. ICT-related tools) and interoperability systems **for communication** that should improve data exchange among partners during a crisis, thus facilitating cooperation between different organisations and improving crisis management and efficiency. These projects are responding to the growing use of ICT within end-user organisations and the simultaneous fragmented nature of these end-users.

  For instance, the **IDIRA** project focused on setting up an IT system that would reinforce interoperability among different communication systems, thus enabling crisis management authorities to gather data coming from different partners. Another project, **IMPRESS,** aimed to advance the response capabilities of a range of emergency medical services through the development of a Decision Support System that would enable the rapid collection of relevant data and the exchange of information between multiple sources.

- A group of projects deals with the **development of different individual tools**, from decision-making support tools to very specific tools that could be used for detection and protection. For instance, the **INDIGO** project focused on the development of a virtual reality-based system for crisis management, while the **IF-REACT** project focused on developing protective clothing for first responders.

- Some projects focused on the **development of toolboxes**. These gather different **tools, methods, guidelines**, etc. that can help first responders to choose the most appropriate means to deal with the issues they are facing. Development of these toolboxes is seen as an efficient way to raise awareness among policy makers and end-users of existing technologies and resources and provide them with guidelines regarding ways to combine them.

  This group of projects includes "Phase I" (e.g. ACRIMAS) and "Phase II" (e.g. DRIVER) **demonstration projects**, which are dedicated to the presentation and integration of existing or newly developed solutions for improving capabilities of European organisations to respond to crisis. **CATO**[164] and **PRACTICE** are examples of projects dealing with the development of toolboxes that should help authorities to develop their own framework to deal with CBRNE-related crises.

[161] http://cordis.europa.eu/project/rcn/98969_en.html

[162] http://cordis.europa.eu/project/rcn/185488_en.html

[163] http://cordis.europa.eu/project/rcn/111121_en.html

[164] http://cordis.europa.eu/project/rcn/102095_en.html

F.9.3 Involvement of end-users

End-users are the main targets for the common tools, methods and resources being developed through these projects. The engagement with and involvement of these stakeholders within projects is therefore important for ensuring the usefulness and applicability of the results and outputs.

Among the 42 projects assessed, just two are **coordinated by an end-user organisation:** OPSIC, coordinated by the Danish Red Cross (first responder); and FAST-ID, coordinated by INTERPOL (police forces). In the latter, the involvement of INTERPOL resulted from its own resolution calling for the creation of an international missing person and unidentified bodies database.

Most other end-users participating as partners in the projects fall into two main categories: **emergency services** (including fire and rescue services, emergency medical services, etc.) and **public security services** (police forces, national authorities responsible for health, defence or police issues, etc.). Overall, these end-users represent around 13% of participants in the projects, and around 8% of total costs or EU contributions. Indeed, the average EU contribution per end-user is around € 35,000, substantially below the € 57,000 per participant generally.

End-users are also involved in the projects through other means, such as through interviews, newsletters, advisory groups, and participation in workshops or demonstration activities.

The objectives of (direct or indirect) involvement of end-users in projects include:

- The identification of end-users' **needs**;
- The definition of **requirements** regarding tools, methods or guidelines;
- The collection of **feedback** on developed products or services.

Involvement of end-users in these projects is also considered as an efficient way to reduce time-to-market and to raise awareness in relation to the new resources.

F.9.4 (Expected) results and outputs

Only half of the selected projects were due to have completed at the time of writing, and many of these were only recently concluded. This means that evidence on outputs and impacts can only be partial. However, according to the stakeholders consulted for this case, most projects have so far been successful in achieving at least parts of their goals. Some examples of results and impacts already seen include the following.

Prototypes - for interoperability systems, decision-making support tools, tools for first responders, etc. often complemented by guidelines or training protocols, aimed at easing the integration of prototypes into the first-responders' portfolio of tools and methods. These prototypes should lead to products in the future, but only if a partner or a client decides to dedicate time and budget to it.

For example, the **FAST-ID** project developed an international database for missing persons and unidentified bodies (MP/UB), as well as the prototype of a standardised system to automatically match missing persons and those discovered injured or dead at disaster sites. The system was successfully integrated with a test platform to validate the possibility for users and officers in member countries to access it through Interpol's existing portals and systems. Interpol has prepared an MP/UB implementation plan to implement the FAST-ID prototype at a production-level scale, and is currently seeking funding to progress this work. Full-scale implementation would aid international police cooperation in the identification of missing persons, unidentified bodies and persons unable to identify themselves for both disaster victim identification and also during daily police work.

Toolboxes, technological frameworks and guidelines - these types of outputs rely on multiple tools, methods and resources. They should help end-users to define their needs, to gain a shared sense of what is at stake and what can be done with existing solutions to improve interoperability, they can also help to organise multi-agency responses.

For example, the **CATO** project developed a comprehensive Open Toolbox for dealing with CBRN crises caused by terrorist attacks using non-conventional weapons. The toolbox contains a knowledge base of scientific and technological information, as well as a comprehensive set of operational guidelines and a decision support system. At the end of 2014 the toolbox was trialled at the Emergency Response Coordination Centre (ERCC) in Brussels, which was set up to support a coordinated and quicker response to disasters, using resources from over 30 countries.

Standard-related activities - Market fragmentation is also a cause for less integration of MS systems. Standard-related activities can push for the adoption of common standards among Member states, thus helping cross-border cooperation and inter-institutional cooperation.

For example, in May this year the **IDIRA** project – which focused on the interoperability of data and emergency procedures in response to large-scale disasters - published a report providing recommendations for harmonisation and standardisation, particularly in relation to information exchange.

Developing common tools or methods from scratch is not always easy or even suitable, as most countries would have their own systems already in place. This is why some projects focus less on developing a common tool and more on creating a common framework or architecture, where national systems can be "plugged-in". These "middle-ground" solutions enable exchanges and harmonisation.

It is also important to note that often clients or end-users cannot directly use outputs from projects, as they demand more work. This can be done for instance through internal projects (CATO, FASTID) or Demonstration projects, in order to turn generic outputs into specific solutions.

The DRIVER project, which is the "Phase II" demonstration project dedicated to crisis issues, has only recently started. It will be significant for the integration of crisis-related solutions and also for exchanges among end-users. The DRIVER project is also pushing for integration and interoperability rather than radical change through the adoption of a common unique tool. It has started to work on the issue through its involvement in a European First Responders Interoperability workshop.

F.9.5 Challenges

Stakeholders consulted for this case have identified several challenges that can reduce the potential impacts of the projects under examination. Some of these issues could equally well apply to projects in other parts of the Security programme.

A central challenge for these projects is **to address the relevant stakeholders** – which are often policy makers at national or EU levels (in charge of setting up requirements, organising public procurements and drafting legislations) and end-users (that will integrate these solutions in their portfolio). Even if most projects engage with end-users and policy-makers in one way or another, the timing and channels used are not always the most appropriate, e.g. too late in the project or not directed toward the DG in charge of the issue. Consortia also often ignore (or are ignorant of) how the policy cycle works and do not know the priorities of political institutions.

One of the objectives of these projects is to **develop a common understanding of an issue**, in order to develop a common tool or method, that could be developed in different countries and improve cooperation capacities. However, cooperation can be difficult, especially between different types of end-users, as they have different professional cultures and different expectations. This can be even more difficult to include them in the process when end-users are mostly volunteers, as it is the case in different countries in crisis areas (e.g. Red Cross in Germany and Austria). Most of end-users have also limited experience in participating to FP7 projects or R&D projects, as they do not have an R&D or a research department. Involvement of end-users through project advisory boards, or workshops and demonstration activities are often solutions used by consortia to gain insights from end-users.

Other identified issues included:

- Ensuring synergies and exchanges between projects is important, given the inevitable crossovers between the activities, outputs and target audiences of different projects.

- Even if Security Research Actions are market-oriented, it might take more time than the period the project covers to develop a product or a solution to a stage that is market-ready. It is therefore often down to individual project partners to work on the outputs further once the project has concluded.
- Public information on projects (e.g. on websites) is not always available or kept up to date, which may be preventing potential users or developers making the best of available results.

F.9.6 Conclusions and lessons learnt

This case has shown that a large number of FP7 Security projects have contributed to the **development of important new tools**, methods and resources that could help to reduce fragmentation and improve interoperability. These new or updated solutions are likely to help to improve the efficiency of response in case of (cross-border) crises.

However, it **will take more time to fully assess the impacts** of these projects on security capabilities and gap reductions in the crisis field, as most projects are just being completed or will end in the next two years. Moreover, as many projects are developing prototypes or generic solutions, it will take further work to move these "pre-solutions" to market and ensure (common) use in the future.

Lessons can be learnt from these projects and the **difficulties they have faced**, in order to increase the impacts of future projects dealing with similar issues:

- End-users should have a central role in projects, be consulted as early as possible and be associated with each step in the project. This is the best way to avoid gaps between their needs and project activities.
- More efforts are needed to address DGs' policy priorities and to close the gap between policy level and technical /research levels. It is important that consortiums gain a more comprehensive understanding of the political agenda and the way they can interact with European Commission DGs or national authorities – in order to avoid duplication of work and increase the impact of research projects.

The European Commission has started to set up **Communities of Users**, in order to e.g. map projects that are investigating common issues and to raise awareness within the community of what is going on in other projects. This is important and should be developed in the future, as it might allow for less overlaps and a more efficient dialogue between consortia and DGs. This could also be done through more systematic common workshops or meetings. It will also be important to encourage a more efficient organisation of end-users at EU level, in order for them to better formulate their needs and increase the dialogue between them and projects. User communities are looked at in more detail in a case on shaping the end-user landscape.

F.10 The involvement of the citizen in security research

The focus of **this case study** is the involvement of citizens in security research in the Seventh Framework Programme, contributing to the evaluation of the effectiveness of the FP7 Security Research programme in terms of reaching intended target groups and the potential impact and added value from citizen involvement.

First, the case study will consider the extent to which citizens and Civil Society Organisations (CSOs) genuinely participated in the Security Research Actions and in what kinds of projects. It will then reflect upon the purpose of the involvement of citizens, if there were any gaps, what the challenges of engaging with citizens are and how they are overcome. Subsequently, it will address the impact and advantages associated according to project participants and see how the project results were disseminated and if they reached the relevant community before finally drawing conclusions for the future of security research.

The case study relies on a review of academic literature, analysis of documents and data from FP7 Security Research Actions, analysis of preliminary results from the SecurePart project – including data on the participation of CSOs in FP7 Security Research Actions – and a series of interviews with representatives from five FP7 Security Research projects and the European Commission.

F.10.1 Introduction

More than other research themes security depends on the acceptance or tolerance of research results by citizens. Security of the citizen includes the protection of the citizen, but, to be effective, also encompasses issues such as privacy, dignity and liberty of individuals. The issue of citizen engagement with the Security Research Actions is important as there has been **some criticism** as regards the poor record of citizen engagement with the Security Research Actions. For example:

- In a 2011 submission to the European Commission's consultation on an Industrial Policy for the Security Industry, **State Watch** complained that the development of the security research programme had favoured the interests of the defence and security industries over the concerns of civil society and other stakeholders. It claims that the EU security research agenda has been strongly influenced by the representatives of corporations from the defence and security industries[165] and that "*successive ad hoc advisory bodies established by the European Commission (the Group of Personalities, European Security Research Advisory Board and European Security Research and Innovation Forum) have all been dominated by industry stakeholders and perspectives*".
- The **interim evaluation** of FP7 Security Research in 2011 found that there was only limited direct involvement of EU citizens in FP7 security research projects[166].
- A recent article by a **social scientist** claimed that the stakeholder involvement in the policy formulation process has established a high-tech bias in the research agenda of the SRA led by a market-oriented, industry led paradigm and a disproportionate power dimension[167].

[165] Submission by Statewatch in response to Section 4 ('Securing the citizen and the society') of the European Commission's consultation on an Industrial Policy for the Security Industry.

[166] CSES (2011) Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research. Sevenoaks.

[167] Kolliarakis, G. (2014) Of Wolves and Sheep: CSO Participation as a Responsible Research and Innovation Mechanism in European Security Research. *In:* Brodersen, S. et al. (Eds) An Innovative Civil Society: Impact through Co-creation and Participation. Copenhagen.

- A 2014 study reviewing "Security Measures in the 7th Research Framework Programme FP7 2007-2013" for the **LIBE Committee** found that funding has been overwhelmingly devoted to security and defence programmes of large transnational corporations, Ministries of Interior and Defence and technical research institutions, with little funding for data protection, privacy and the respect of fundamental freedoms in security applications. The authors commented that security research has only partly addressed the concerns of EU citizens and society.[168]

The **definition of citizen involvement** within this case study has tried to focus upon individual citizens not exclusively as representatives of organisations, although some consideration of Civil Society Organisations (CSOs) and their participation in the FP7 SRA has been made.[169]

There are political and practical **reasons for a close involvement of citizens** in security research:

- **Political arguments** for the security of the citizen include not only the protection of the citizen but also encompass issues of privacy, dignity and freedom of individuals.
  - Security is not a straight forward issue and it is often acknowledged that in order to protect individuals their freedoms and liberties are compromised. Identifying some feature of the world as a security issue is to grant it a particular privileged political status and to start to frame the issue in a specific way, deserving political and social responses and identifying it as the responsibility of certain political actors.
  - Security practices, including research and innovation, can contribute to the normalisation of security[170], with security becoming an organising principle across many areas of social life, sometimes to the detriment of other values or principles, such as, for example, privacy, transparency, freedom of speech or the democratic process[171]. This tension between security and freedoms represents a crucial aspect and challenge in the FP7 Security Research Actions. Subsequently it can be argued that any work undertaken to improve the security of the citizen should carefully consider the views of citizens in the design of any security related technology product or process.
- Beyond the political arguments for citizen involvement in security research there are also more **practical reasons** for the consideration of citizens and their views in Security Research Actions.
  - New technologies require **acceptance** for adoption by the populace and participation in the process of development can help citizens to shape technologies they trust.
  - A further reason to critically reflect upon the involvement of citizens in the Security Research Actions of FP7 is the fact that citizens can potentially make **valuable contributions** to research and innovation in the security field. Citizen engagement in research is reported to add value to research activity in a number of identifiable ways. A few examples include the promotion of divergent thinking, which helps to find novel solutions to complex problems. Diverse perspectives from a range of actors involved in a research activity can add specific value when teams are trying to solve difficult problems. People with different perspectives have different 'heuristics' or methods and tools for

[168] European Parliament (2014) Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013. Study PE 509.979. Brussels.

[169] Representatives of CSO, as well as researchers are citizens too. However, their participation in research projects is based (legitimized) on their organisational membership and expertise (functional roles) and not the mere fact that they are citizens. Moreover, it can be assumed that their motivation is *primarily* guided by their functional roles rather than by a concern for the public, which is not to say that researcher and CSO representatives are not concerned about the public weal, just that their functional roles take precedence or are at least an additional factor when it comes to matters of motivation and judgement. A citizen is assumed to be responsible only to her consciousness.

[170] Nissenbaum, H. (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life,Stanford Law Books, Stanford, p. 161.

[171] Barnard-Wills, D., Wadhwa, K., Wright, D. (2014) Social Impact Assessment Manual and Toolkit. ASSERT Project. European Commission – 7th Framework Programme, Brussels: European Commission.

finding solutions. Diversity is especially important where the problem at hand is complex: if only experts with similar perspectives and heuristics are engaged in the process of problem solving, then they are likely to 'become fixed in the same places'. A more diverse group of problem solvers will not.

- Citizen engagement can increase the **legitimacy** of projects and decisions. Where citizens have been involved in the design, development and implementation of a social innovation or in a decision making process relating to that innovation, the innovation is more likely to be seen more legitimate than if it had been developed without such a process.
- Citizen engagement is **necessary because of the nature of the social challenges** faced by humanity. Of particular relevance to security research many of these social challenges are 'wicked' or complex problems that defy linear, top-down policy responses and addressing many of these complex challenges requires behaviour change. Terrorism and cyber security are both examples of 'wicked' problems that are difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognise and that operate in shifting environments. These types of problems do not stand still and solutions to wicked problems therefore cannot be delivered in the way that commercial products are delivered – they require the participation, co-operation and 'buy in' of users.[172]

The **research conducted for this case study** is based on three streams of data collection:

- Preliminary results of the FP7 SecurePart project, which addresses the issue of broadening societal participation in security research. The SecurePART project aims at enhancing the influence of civil society in formulating, monitoring, and implementing current and future EU security research."[173]
- Data and document analysis of FP7 Security Research Actions that involved citizens in the project work. Data for the entire Security Research programme detailing the extent of engagement by projects with individual citizens is not available. However based on publicly available data from project SecurePART there are less 80 CSOs that can be identified as beneficiaries of the Security Research Actions, which corresponds to roughly to 4% of all participants. However, this level of data does not really allow for an in-depth understanding of citizen involvement and, hence, a number of interviews with selected projects were conducted.
- Interviews were conducted with actors from different security research projects (SecurePART, SURPRISE, FIDELITY, ESS and HEMOLIA) that were particularly useful to identify empirical mechanisms for the participation and involvement of citizens.

F.10.2 Analytical framework – ways of involving citizens in security research

<u>European security research programme policy cycle</u>

In order to help evaluate the involvement of citizens in the Security Research Actions it is useful to first clarify the process and actors involved in the **policy cycle** of the European Security Research Actions:

- The FP is approved by the Parliament and the Council in a co-decision process, which takes place at the beginning of the seven year duration of this programme.
- Under FP7, the European Commission regularly issued a work programme, to implement the Cooperation Specific Programme and its themes, setting out in greater detail the objectives, scientific and technological priorities, the funding scheme to be used for the topics on which proposals are invited, and the timetable for implementation.

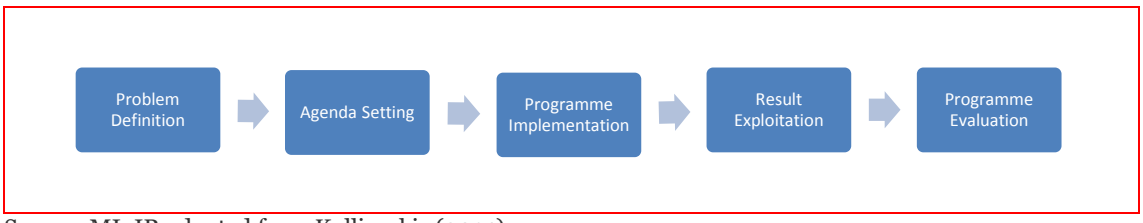
[172] Davies, A and Simon, J, (2012) The value and role of citizen engagement in social innovation. A deliverable of the project: "The theoretical, empirical and policy foundations for building social innovation in Europe" (TEPSIE), European Commission – 7th Framework Programme, Brussels: European Commission, DG Research and Innovation.

[173] http://cordis.europa.eu/project/rcn/185508_en.html. In addition, the CONSIDER project addresses issues of citizen involvement in security research.

The content of this work programme is subject to the preliminary binding opinion of a **Programme Committee**. This Programme Committee comprises representatives of each of the 28 EU Member States plus the Associated States, and these representatives are from Government Authorities usually Ministries of Research or Ministries of the Interior.

In addition there was a FP7 **Security Research Advisory Group** that could make non-binding recommendations, for instance towards programme implementation but also for future Framework Programmes. The figure below illustrates the policy process. Drawing on Kolliarakis' model of the European security research programme policy cycle five main stages can be distinguished.

Figure 30: European security research programme policy cycle



Source: MIoIR adapted from Kolliarakis (2014).

Within each of these stages, various levels and types of engagement that citizens may undertake in the Security Research Actions can now be identified. Drawing also on the preliminary results of the SecurePART project a number of roles of citizens (and CSOs) in Security Research Actions can be discerned. Citizens can participate in security research as:

- Project participants (actors of research and innovation and dissemination);
- Citizens addressed by project activities (e.g. in surveys or test runs or dissemination);
- Members of project advisory boards (scientific advisory boards, ethics advisory boards, security advisory boards);
- Proposal evaluators;
- Observers of proposal evaluations;
- Project reviewers;
- Members of the Programme Committee;
- Members of the Programme Advisory Board;
- Experts and members of high-level panels for programme evaluation activities;
- Commissioners of research.

Forms of citizen engagement through the phases of the policy cycle

Problem definition stage and agenda setting stage

The quality, relevance and effectiveness of EU policies depend on ensuring a broad participation by citizens throughout the policy chain — from conception to implementation. Improved participation is likely to create more confidence in the end result and in the institutions, which deliver policies[174]. For consultation to be equitable, the Commission should ensure adequate coverage of the following **target groups** in a consultation process:

- Those affected by the policy;
- Those who will be involved in implementation of the policy; and/or
- Bodies that have stated objectives giving them a direct interest in the policy[175].

[174] COM(2001) 428.
[175] COM(2002) 704.

The aforementioned study for LIBE states that relatively few of the participants of these groups came from research or civil society organisations and the forums went beyond their advisory role and contributed significantly to framing the orientations and priorities of EC-funded security research.

Programme implementation stage

In the programme implementation stage the means by which security research projects engage with citizens may be diverse but provides citizens with predominantly a passive role, as in most cases individual citizens are an object rather than a subject of security research. Active involvement of citizens as subjects during this stage can take **different forms**, as it may be:

- Through consultation processes such as citizen summits (as for example in the SurPRISE project), focus groups, or workshops,
- As providers of data through large scale surveys (project PRISMS) or provision of biometric data (project FIDELITY),
- As a part of an audience in a field trial (project ESS), whereby the sub-form of involvement can vary considerably,[176]
- As members of project advisory boards (scientific advisory boards, ethics advisory boards, security advisory boards),
- As individual experts who evaluate project proposals, or
- As individual experts who review project results in post award stages in the context of periodic and final project reviews.[177]

Project **advisory boards** are composed of individual citizens with specific expertise in a given field. For instance, ethics advisory boards are composed of experts having in-depth experience in ethical questions. Experts in advisory boards could come from any kind of organisation, depending on the nature of the board. This includes universities, research organisations, industry and civil right organisations.

In comparison to individual citizens in the roles mentioned above, citizen representative organisations such as CSOs can also be full participants in a **research project**.

Results exploitation stage

At the results exploitation stage citizens and CSOs may be engaged as disseminators, invited into project consortium to play the role of a **broker** to the world outside of the research action. Preliminary results from the on-going SecurePART project suggest that CSOs are invited into project consortia as beneficiaries mainly to play the role of disseminator, as the broker to the world outside.

Programme evaluation stage

"Evaluation" refers here to the evaluation of the Security Research Programme overall, as part of FP7 (as opposed to the evaluation of proposals and the review of projects), in particular its relevance, efficiency and impacts. Evaluations of Framework Programmes are usually carried out by a high-level panel, supported by evaluation activities, for instance studies, in the various Framework Programme Themes. These studies are usually carried out by private and/or public organisations that are tasked by the Commission. Representatives of CSOs or individual experts might be **consulted** as part of the stakeholder consultation process that usually forms part of an

[176] For example, the projects can hold focus groups of ordinary consumer-citizens or can conduct surveys by telephone or e-mail or face to face; they can post the project description on the organisation's website and invite comments; they can hold public hearings where they describe the project and invite comments from the audience or from experts and then invite comments after the experts have spoken; they can prepare stories or adverts in the media and invite comments from readers; finally, project can also conduct Delphi surveys of experts, to query them on potential societal risks now and in the future.

[177] In the latter two cases, citizens volunteer through the European Commission's Research Participant Portal to be registered in the experts database to evaluate or review or monitor projects in their field of expertise. This is not for lay persons but for scientists/researchers. Experts are then selected by the European Commission to undertake the work.

evaluation. However, both types of actors and in particular the citizens do not form part of the usual group of people addressed through surveys, workshop discussions or interviews in programme evaluations.

To **summarise**, the brief phase-based consideration of the engagement with citizens in FP7 SRAs shows that citizens are in general rather objects of security research than subjects.[178] The analysis identifies the implementation phase as the one where citizens are most widely involved as subjects of research through various activities described above. Compared to individual citizens, CSOs could be engaged at an earlier stage and more intensively in the consultations about the security research agenda.

Examples of mechanisms for the involvement of citizens

A range of mechanisms employed within the projects for the engagement of citizens during the implementation phase were identified. The examples detailed below include citizen summits and large scale field trials.

In the **Emergency Support Systems (ESS**) crisis management project (2009-2013)[179], a range of **field trials** was run to test and directly engage with citizens. The objective of the ESS project was to develop a suite of real-time, data-centric technologies focused on providing web-based actionable intelligence to crisis managers during atypical event scenarios. The aim was to enable improved control and management, resulting in real-time synchronisation between forces on the ground (police, rescue teams and fire fighters) and out-of-the-theatre command and control centres.

The project consortium used **real-life testing** of the ESS framework products and technologies for real-life crisis management situations. Examples of the field trials included a simulation of a flood event crisis, cross-border (Italy-France) air-crash incident in the mountains followed by a mass forest fire, and an accident involving a truck carrying dangerous chemicals leaching to a nearby river.

Figure 31: Flood event crisis field trial

On 24th March 2012 at the Stade des Costieres in the city of Nimes (F) the ESS security action research project ran a field trial based on a scenario concerning a flood event crisis in the area where the Stade des Costieres is located.

The purpose of the event was to demonstrate and validate the potential contribution and performance of the ESS system to crisis management operations. The test was organised by CEREN, the Test and Research Center of ENTENTE for the Mediterranean Forest, on behalf of the ESS consortium in cooperation with local and regional services and authorities including Nimes Prefecture, Gard Department Fire Service, Police, City of Nimes, Meteo-France and Autoroute du Sud de la France.

The location was a football match at the Nimes Stade des Costieres. On ticket purchase audience members were provided information about the simulation experiment. During the match the project team sent audience members a text message to their mobile phones asking them to behave in a specific way and to participate in a mass evacuation due to floods.

Source: Summary based on publicly available information from the project website

The **SurPRISE project**[180] describes itself as a large-scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe. An emergent body of work has suggested that the trade-off argument of security versus privacy has over-simplified how the impact of security measures on citizens is considered in current security policies and practices. Thus, the more complex issues underlying privacy concerns and public

[178] In this context please note the remark on the fact that representatives of CSOs and researchers are citizens too, made above in footnote 67.

[179] http://cordis.europa.eu/project/rcn/91016_en.html

[180] http://cordis.europa.eu/project/rcn/102076_en.html

scepticism towards surveillance-oriented security technologies may not be apparent to legal and technological experts. This project tackled directly this issue of the security-privacy relationship and citizen involvement in this research was a core activity of the work programme.

The SurPRISE project employed two main mechanisms for citizen participation – a **citizen summit** and a number of smaller, half-day events with approximately 40 participants. The active engagement involved approximately 2,000 citizens from 9 European countries in participatory assessment activities. The citizen summit will be briefly presented here due to its rather innovative character of citizen involvement.

Figure 32: Citizen summits as a mechanism for the involvement of citizens

Citizen Summits: The SurPRISE project explored the relationship between security, surveillance and privacy. As part of the methodology to investigate this issue, the project used a mechanism of large scale citizen consultations to engage European citizens in the research and to learn more about their views and opinions on surveillance, privacy and security.

'Citizen summits' were held in 9 European Countries in 2014 to give people the opportunity to meet and discuss specific security technologies and their implications. These "Citizen Summits" involved on average about 200 citizens per country.[181]

All citizens participating in the summits received an information booklet before the event. This booklet contained information about 3 surveillance-oriented security technologies: deep packet inspection (DPI); smart closed-circuit television (CCTV); and smartphone location tracking.

Participants who attended the citizen summits discussed two of these technologies. These were whole day consultations incorporating the showing of a short documentary file presenting the pros and cons of technologies for discussion during the day. All participants received electronic voting devices called clickers. These were used after discussion rounds to answer questions about attitudes towards the technologies. The questions were shown on a big screen at the front of the room. The last discussion round aimed at reaching a consensus at each table for a recommendation to present to European policy makers.

Source: Summary based on publicly available information from the project website

The **FIDELITY project**[182] aimed to analyse shortcomings and vulnerabilities in the ePassport life cycle, and to develop technical solutions and recommendations to overcome identified issues. The subject matter of this project is of concern to any citizen as there is a direct impact on them if there are changes to tools or processes.

The main mechanism to involve citizens in this project was a call for volunteers to contribute biometric data to help the project team construct a temporary database for biometrics. They were subsequently used for testing the algorithms developed by the project. In other words, the citizen engagement within this project took the form of providing data (biometric data) rather than contributing to any consultative activity.

The PRIvacy and Security MirrorS (PRISM)[183]: The PRISM project aimed at developing a framework for integrated decision-making and approached its main questions through a large-scale survey among European citizens. Between February and June 2014 around 1,000 telephone interviews in each EU Member States except Croatia (27,195 in total) were conducted using a representative sample (based on age, gender and work status) within each country.

The survey explored **respondents' perceptions of privacy and security issues** and values questions including political views, attitudes to rights and perceptions of technology. The core of the questionnaire, however, was a series of eight vignettes aimed to understand public opinion

[181] "Citizen summits are full day events with alternating phases of receiving information, discussing emerging issues in small groups, electronic voting on general aspects of the relation between surveillance and security and on specific surveillance technologies, and of developing recommendations from the citizens to policymakers." Strauss, S. (2014) D 6.10 Citizen Summits on Privacy, Security and Surveillance: Synthesis Report. SurPRISE project.

[182] http://cordis.europa.eu/project/rcn/102324_en.html

[183] http://cordis.europa.eu/project/rcn/102282_en.html

towards different privacy and security scenarios. The questions for each vignette included whether the practices described should be allowed; the impact on people's rights and freedoms; and a series of specific statement questions about each vignette.

The broad **methodology** of the PRISMS project incorporated the use of interviews, focus groups and workshops which brought together various stakeholder groups including citizens, policy advisors, security people, societal organisations, criminologists and scientists.

These examples show the variety of mechanisms that FP7 funded security research projects used to engage citizens in their activities. In these examples citizens have been part of field trials and thereby objects of research, they provided data for research, or commented and reflected upon the research. Each of the mechanisms discussed is linked to a number of challenges, which will be discussed more generally in the next section.

F.10.3 Challenges to engaging citizens

There are a **number of challenges** to the involvement of citizens and CSOs in the implementation phase. The following is not an exhaustive list but rather highlights the concerns that were raised during the research for this case study.

- **Not all projects are equally suited** to involve citizens in the implementation phase due to the nature of the project or its research topic. For example, there can be confidentiality issues that limit the possibilities to involved citizens. Also, project deliverables or results may be classified (i.e. represent EUCI = European Union Classified Information, where specific rules and conditions apply). In general, however, there are topics that are suitable for a systematic consideration of the involvement of citizen. One example is the field of crisis management, which is generally concerned with the population at large and for which the ESS project has successfully demonstrated the use of citizen involvement.
- The case study found that there is a level of unfamiliarity among projects about how best to **contact and include citizens** in research. This concerned numerous rather simple issues such as
  - Where to go, i.e. which authority/organisation to contact that can represent citizens that can be approached;
  - How to reach citizens due to a lack of awareness of the EU's research framework programme amongst the general public;
  - How to ensure a representative sampling of citizens;
  - How much time and budget to reserve for such an effort. The practicalities and additional complexity and cost of a more interdisciplinary approach to the work can be a significant deterrent to a more participatory approach to security research.
- The involvement of **Civil Society Organisations** in security research projects comes with a similar set of challenges.
  - One issue concerns the definition of a CSO and it statistical identification. For example, the Red Cross, which is involved in projects such as SPEEDKITS through their shelter research unit in Luxembourg, has a four-fold role as researcher, end-user, quality manager and steering committee member in that project. The Red Cross more generally in SRAs is primarily an end-user of security research. At the same time it is, like other similar organisations, a CSO. This question might appear rather miniscule but also has effects on the statistics.
  - To what extent do CSOs represent the public interest? The SecurePART project found that the CSOs themselves say they are not representing the public interest per se and that they have a particularistic agenda. They could be engaged in that sense as lobby groups with the difference that they are not for profit and that their agenda touches on civil rights, civil liberties and welfare, which is not the case with many other lobby groups. The legal definitions do not help to disambiguate between different types of CSOs. There are trade and professional associations such as the European Organisation for Security (EOS), which is a major lobby group and also non-for-profit but there are

also RTOs such as Fraunhofer, TNO, which a lawyer would define as CSOs. The issue here is the boundaries of operational definitions in the policy realities.

While these issues are not insurmountable barriers to the involvement of citizens or CSOs in security research projects, they point to challenges that projects teams have encountered. These challenges identify, on the one hand, possible remedies and on the other, point to the importance of knowing the impact associated with the engagement of citizens in security research projects.

F.10.4 Impacts of engaging citizens

In addition to the benefits of engaging citizens the interviews conducted for the purpose of this case study point to further positive impacts of the involvement of citizens. Among the benefits cited by interviewees are the following:

- Involving citizens generates material for **new research questions** and ideas. The SurPRISE project is particularly pertinent to this case study as it re-examined the relationship between security and privacy, which it describes as 'commonly positioned as a 'trade-off''. In the SurPRISE project one dimension of the large scale events used to engage citizens was to try and establish the reasoning behind the opinions and recommendations of the citizens, in relation to security or security measures and also to develop a model and criteria of the acceptability of security or surveillance technologies. The output was a wealth of information on the issues surrounding surveillance technologies with some predictable results but some that were more unexpected. Both led to the identification of novel research questions. Citizen participation is perceived to provide added value by broadening the initial framework or focus of the research away from that of the original consortia architects.
- In the introduction to this case study it was noted that security is not a straight forward issue and it is often acknowledged that in order to protect individuals their freedoms and liberties are compromised. This **tension between security and freedoms** represents a crucial aspect and challenge in the FP7 Security Research Actions. The results of the SurPRISE citizen summits show that participants do not follow a trade-off argumentation: citizens neither want to fear security measures nor lose their privacy. Hence, they deem the trade-off between privacy and security inappropriate, both with regards to the effectiveness of security measures as well as the protection of privacy. Instead of a trade-off, alternatives are needed with respect to the effective protection of their privacy which was seen as a *sine qua non* for the acceptability and effectiveness of security measures[184]. The engagement and feedback from citizens in the SurPRISE project could help to shape the future research agenda, specifically in the area of surveillance.
- Moreover, involvement of citizens can help to **achieve better security solutions**. For example, the SurPRISE project identified advantages for ergonomics and process design based on the feedback on the day-to-day lives of citizens. Furthermore, countries and cultures throughout the EU represent different approaches to security, and acceptable measures in one country will not be the same in another. The Member States do not have a homogenous administrative approach as illustrated in Belgium, for example, where there is a central database of the whole population who are all registered with a single number, compared with Portugal where the population opposes this type of registration. Designing for people in a pan-European setting has to take into account the variations in views across the Member States and consultation with citizens helps to elaborate the context. Similarly, the field trials of the ESS study described above provided feedback from large-scale simulation experiments.

These empirically identified benefits of engaging citizens add to the list of positive aspects outlined above and drawn from the academic literature.

[184] Strauss, S. (2014) D 6.10 Citizen Summits on Privacy, Security and Surveillance: Synthesis Report. SurPRISE project.

F.10.5 Conclusions and lessons learnt

This case study has investigated the engagement of citizens in the FP7 Security Research Actions, which is a complex and multi-faceted issue. Inevitably, a short case study such as this can only generate a first approach towards a complex and multi-facetted issue. The focus has been on the participation of individual citizens with passing reference to the participation of Civil Society Organisations.

The results of this case study suggest that **citizens are under-represented** in the FP7 Security Research programme. This point is equally made in the academic literature[185], the interim evaluation of the FP7 Security Research Actions,[186] as well as several reports from CSOs and the European Parliament[187]. Based on an analytical framework that distinguished different phases of a security research policy cycle, four stages to engage citizens in security research have been identified. It is an engagement that mainly happens in the implementation, exploitation and evaluation phases of projects rather than at programme level.

At the **project** level, as this case study points out, the engagement of citizens and CSOs is **rather limited** and is not really contributing to shaping the technologies being developed. In other words it is post hoc after the research design is in place and often even after the results have emerged. Moreover, citizens are engaged in FP7 Security Research Actions predominantly as an object of research and to a much lesser extent as active research subjects.[188]

Interviewees from research projects at the programme implementation phase speak **positively about the results of engaging with citizens**, but questions remain about the extent of actual involvement, the quality of the engagement and the practicalities of genuinely including citizens and their views in the Security Research Actions. Direct engagement with citizens is viewed by project respondents as positive for the outcomes and the impacts of their work, but they raise a number of questions about how best to maximise the potential of future interactions with this group.

Based on these conclusions of the case study, the following **recommendations** with regard to future security research are offered:

- The Commission should **encourage security research projects to engage with citizens**. There are a number of ways to foster such a development.
  - A priority would be to consider carefully whether a topic of the work programme would benefit from direct citizen participation and if so, to include it in the **requirements and the evaluation criteria**.
  - The case study has pointed to a number of **practical mechanisms** used effectively for citizen engagement by projects. These should be collated systematically and made available in an information source for project applicants to draw upon, for example through a web page specifically devoted to the topic of citizen engagement in SRAs, successes, benefits, challenges and how those challenges can be overcome.
  - This list of appropriate instruments should be further broadened by a more in-depth study on this topic and made available to security research action applicants in order to facilitate their projects. There are also current EU-funded **research** projects, which are working to produce structured methods for consultation in the decision-making of research policy. Under the heading of "citizen science" another strand of research funded by the Commission develops methods to have citizens actively take part in the

[185] Kolliarakis, G. (2014) Of Wolves and Sheep: CSO Participation as a Responsible Research and Innovation Mechanism in European Security Research. *In:* S. Brodersen et al. (Eds) *An Innovative Civil Society: Impact through Co-creation and Participation*. Copenhagen.

[186] CSES (2011) Ex-post Evaluation of the Preparatory Action on Security Research (PASR) Interim Evaluation of FP7 Security Research. Sevenoaks.

[187] European Parliament (2014) Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013. Study PE 509.979. Brussels.

[188] In this context please note the remarks made in footnote 67 above.

research work, thereby turning them into subjects of research[189]. The results of both types of projects should be linked to European security research at programme and project levels.

- Furthermore, the Commission should investigate ways to involve of citizens at **programme level**.
  - For example, citizens should not only be involved for collecting data or be consulted to validate existing findings, they should also participate in **shaping the work programme**. This kind of involvement might help with later acceptance of a developed security solution, product or service. As Statewatch note there is '*growing public concern about the development and implementation of a range of new security technologies such as biometric IDs, risk profiling and the use of surveillance 'drones'*[190]'. If the Commission and the security research community are to avoid further costly experiments such as the introduction of full body scanners at UK airports then some genuine citizen consultation at the earlier stages of the policy cycle may be of assistance.
  - Another way to strengthen the role of citizens at programme level would be to strengthen the role of representatives of a larger variety of CSOs in **review of projects**. This would further engage CSO representatives in the process of commissioning research and proposing topics for the upcoming work programme, as evaluation results feedback through the policy cycle.
  - Similarly, the Commission could examine ways to involve citizens in the **dissemination stage**, e.g. through citizen's panels. The latter could be organised directly by the EC. This panel would be gathered for one day to hear the outcomes of projects. Project leaders could explain the research and seek the views of the panel about the work being undertaken and to gather their opinion or consent on emerging results. This would be a broader Commission organised activity rather than a direct project resource based activity.
- Finally, this case study has yielded a range of **emergent considerations** around the topic of citizen engagement in security research, which should be examined in a more extensive manner, when going forward. These concern in particular whether more citizens should be directly engaged in the work programme for the new framework for security research, and – if this is deemed desirable – then how to engage the citizens. Questions could be: Should projects themselves all be encouraged to have a strong component of citizen consultation? Should separate research projects consider citizen views on relevant societal related consequences of technologies or should the Commission run citizen focus groups to consider the new ideas, products and processes emergent from the research projects and wider citizen consultations to shape the work programme itself?

[189] See for example https://ec.europa.eu/digital-agenda/en/citizen-science.
[190] Statewatch (2011) Rethinking the EU Security Research Programme.

F.11 Project clusters – success factors for cross-project collaboration

This case study examines the activities and experiences of the first clustering of projects in the FP7 Security Research Programme, the 'DEMOSEC' cluster of three projects focussed on different aspects of the subject of surveillance. It illustrates how cross-project collaboration and coordination can be approached, and highlights some of the benefits, as well as the challenges, that can result from such efforts. It contributes to the evaluation of the efficiency of the implementation of research projects and the effectiveness of the dissemination of results.

The case will first introduce the subject of project clustering before examining the origins of the DEMOSEC cluster, the rationales and expectations to the cluster, the implemented cluster activities and their benefits, as well as issues and challenges encountered during this experience. The final section will draw conclusions from the experience and offer some lessons for Horizon 2020.

In addition to documentary analysis, the case study draws heavily on consultation with seven key stakeholders, including consortium coordinators and partners from the three projects concerned as well as representatives from the European Commission.

F.11.1 Introduction

Across the Framework Programme there are a number of examples of '**project clusters**' that have emerged around particular topics or challenges. For example, the 'European Research Cluster on the Internet of Things'[191] (composed of 14 FP6 and FP7 projects) or the 'European NanoSafety Cluster'[192] (which aims to exploit synergies between over 35 FP6 and FP7 projects, as well as some related nationally-funded projects). In the latter example, participation in the cluster was originally voluntary, but has since been made mandatory for relevant projects starting after 2009.

Such clusters can serve various purposes. For example, the two clusters mentioned above include the following generic **aims and objectives** between them:

- Facilitate networking between related projects in Europe
- Coordinate research activities between these projects
- Establish synergies between the projects involved
- Avoid duplication of work and improve efficiency
- Provide a forum for discussion and problem solving
- Assure coherence of work in Europe and harmonise methods
- Leverage expertise, talents and resources
- Collaborate to maximize impact
- Facilitate the formation of consensus
- Provide a single voice for discussions with external bodies
- Plan future R&D actions and activities

Clusters can also be used to **increase visibility** for the individual projects involved, their research activities and their outputs, beyond that which could be achieved by the individual projects alone. Visibility is important, both to ensure the legitimacy of the research effort in the eyes of the public, and also to foster the dissemination and uptake of research results, and it is the aim of greater visibility that has been one of the main aspects of the establishment of a small cluster within the FP7 Security Research theme.

[191] http://cordis.europa.eu/fp7/ict/enet/rfid-iot-projects_en.html

[192] http://www.nanosafetycluster.eu/

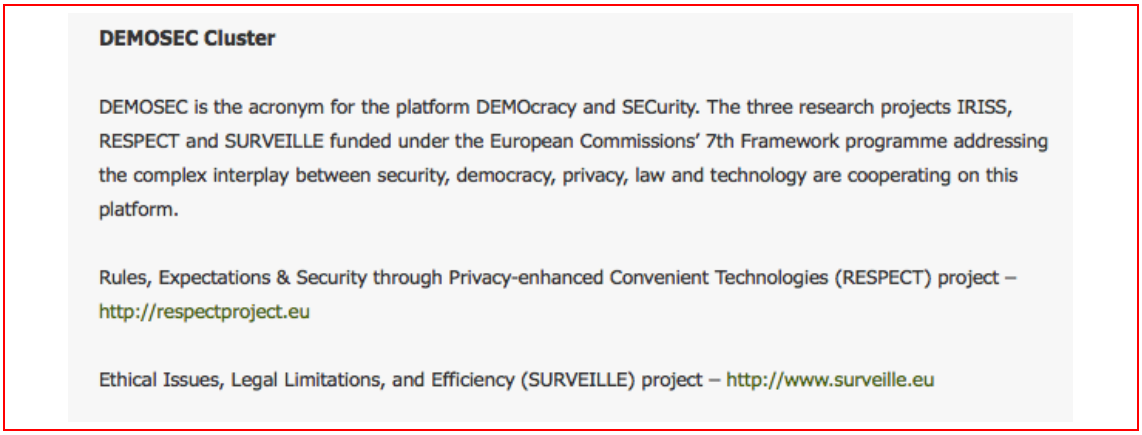
The collaboration in question involved three FP7 research projects (two from the Security Research theme, one from the Socio-economic Sciences and Humanities (SSH) theme) that were addressing related topics around the issue of **surveillance**. These projects were:

- RESPECT: Rules, Expectations & Security through Privacy-Enhance Convenient Technologies (FP7 Security Research Programme)
- SURVEILLE: Surveillance: Ethical Issues, Legal Limitations, and Efficiency (FP7 Security Research Programme)
- IRISS: Increasing Resilience in Surveillance Societies (FP7 SSH Research Programme)

Together they formed a joint platform called DEMOcracy and SECurity (DEMOSEC). However, it appears the term DEMOSEC was merely used as an abbreviation to refer to the three projects as a group (e.g. in the title of the final conference), rather than representing a specific overarching initiative for the cluster.

The DEMOSEC cluster is also presented in different ways by the three individual projects involved. Only the website of the IRISS project explicitly mentions the DEMOSEC platform under 'related links' (see Figure 33; while the RESPECT and SURVEILLE projects do not mention the platform, but do list the two other projects under 'related links'.

Figure 33: Presentation of the DEMOSEC Cluster on the IRISS website



Source: http://irissproject.eu/?page_id=13

F.11.2 Origins of the surveillance cluster

It was the European Commission that initiated the formation of an FP7 surveillance project cluster. The topic was relevant to both the SSH and Security Research themes, and the responsible Commission Services – DG Research and Innovation (DG RTD) and DG Enterprise and Industry (DG ENTR)[193] respectively – decided to coordinate their calls for proposals.

As a result, **two calls** were issued at approximately the same time in the 2011 Security and SSH work programmes, with similar text in each and cross-referencing to the other call. Both provided the same background information on the need to address the topic of surveillance:

> *A range of surveillance systems and technologies have been developed and used by both public authorities and private actors over time, with a peak in the aftermath of the 2001 terrorist attacks. This has also been the case in the EU, and the trend is likely to continue. It is thus necessary to examine the factors underpinning such developments and their implications in terms of actual effectiveness in fighting crime and terrorism, social and economic costs, protection or infringement of civil liberties and fundamental rights and ethical aspects…*

[193] The Unit in charge of the FP7 and Horizon 2020 Security Research meanwhile transferred to the DG for Migration and Home Affairs (DG HOME).

Under the two calls, the specific research topics to be addressed were then further specified:

- In the **SSH** Research theme, a research project was sought that would address how surveillance affects the democratic society and societal values, including the way that surveillance and retention of data may be perceived in different contexts; how human relationships are affected under conditions of visible and invisible surveillance in public and semi-public realms; etc.
- In the **Security** Research theme, the topic aimed at evaluating the impacts of different surveillance systems on the security of citizens. Aspects such as reduction and displacement of criminality, prevention vs. prosecution, efficiency of treatment and storage of information, effectiveness in fighting terrorism, and social and economic costs, were to be taken into account, as well as legal and ethical aspects.

The evaluation of the resulting proposals was also conducted in parallel, and lead to the selection of three projects – all addressing the issue of surveillance from a different perspective, and including explorations of socio-cultural, legal, ethical, technical and operational elements to surveillance.

Following the selection of projects, the Commission organised an initial meeting with the three project coordinators of what would become the surveillance cluster[194], in part to explain the joint activities and interactions that would be required of the three projects. This included: the sharing of deliverables; attendance at each others' main meetings; the organisation of a joint event; and the issuing of a joint policy document.

F.11.3 Rationale and expectations for the surveillance cluster

From the Commission's perspective, the aim of the joint call and subsequent project cluster was to bring together leading experts from different disciplines to look at the topic of surveillance from different angles (technological, legal, sociological), and to provide an opportunity for them to engage and test their ideas against each other. It was hoped that this would result in a more comprehensive overview of what was going on in the field, as well as relevant recommendations for policy-makers, manufacturers and end-users. The requested joint event and policy briefing document in particular were aimed at encouraging the three projects to combine their activities and results in their dissemination to a wider set of relevant stakeholders.

The initiative also functioned as something of an experiment for the DGs concerned. A joint ICT-Security call for proposals (relating to critical infrastructure protection and to technology building for creating, monitoring and managing secure and resilient transport and energy infrastructures) had already been issued at the start of the Security Research Programme, but the surveillance initiative went a step further, by also involving the coordinated evaluation of the resulting proposals and then the setting of requirements for in-project cooperation and collaboration. It was therefore seen as a test case for a more joined-up approach, intended to inform the Commission's thinking about future approaches.

Project partners consulted for this case reported that the Commission's general idea and concept for the joint call was understandable and logical, given the similarity between topics. However, they also suggested that it was not entirely clear what the purpose of the cross-project collaboration then was, or what the Commission was trying to achieve through its requirements for coordinated activities. As a result, those consulted within the consortia tended to regard the surveillance cluster initiative mainly as a contractual obligation imposed by the Commission, and did not appear to have fully bought-in to the need, aims and potential benefits of these activities.

F.11.4 Cluster activities and their benefits

While the call documentation was clear that the implementation of surveillance topics was being coordinated between the Security Research and SSH themes, no explicit mention was made of a subsequent project cluster, or of any foreseen cooperation or collaboration between the projects

[194] The 2011 Work Programme referred only to 'a coordination' with the corresponding SSH topic – the term 'cluster' was only introduced, informally, once the projects had begun.

that would be selected as a result of the calls. The project partners suggested that this did not become apparent until after the projects were selected and the coordinators were brought together for a meeting with the EC – although the project officers concerned believe this was understood at an earlier stage.

The three projects then cooperated through various means, from their inception in 2011 to a final event in October 2014. This included:

- Project coordinators **attending meetings** in their sister projects, presenting their approach to each other and discussing project activities
- The **sharing of key research outputs** and deliverables across the consortia
- A **joint conference**, "DEMOSEC: Democracy and Security", in Brussels in October 2014
- The development of a **joint policy brief** on the basis of the work of the projects

It is clear that some **information sharing** took place between the consortia during the course of the projects, on the approaches foreseen, as well as through various outputs and deliverables that were shared across consortium members.

This was generally information that was (or would be) publically available anyway, but the direct sharing within the cluster does appear to have increased awareness of, and interest in, the information. Some project partners reportedly read the research outcomes from sister projects very carefully and used them to inform (and "nourish") their own work, and did so to a greater extent than might have been the case without this formalised sharing of results between the projects.

At the same time, other partners suggested that little cross-learning took place, even when projects were working on very similar topics. It was reported that there were even examples where two projects had carried out very similar research, but had not collaborated to enhance each others' activities or reduce duplication of effort.

It was the joint **final conference**, however, that was generally seen as the main collaborative activity that emerged from the cluster initiative. Indeed, according to some of those consulted, it was the only real significant joint activity that took place as part of the cooperation between the projects.

The two-day conference served as a joint event for the three projects, with each consortium presenting its results and then contributing to a series of shared panels on cross-cutting topics such as 'surveillance technologies in society' and 'the role of law enforcement agencies in surveillance'.

Project representatives were generally satisfied with the conference, and reported that it was well attended by a variety of different stakeholder groups. They suggested that their project was able to achieve greater visibility, reach a larger audience, have more interesting discussions, and integrate a greater range of perspectives than would have been the case had they just held individual end-of-project events. In particular, for SURVEILLE, the joint conference is likely to have exposed a larger academic audience to their work than would have been achieved otherwise, while for the other two projects, the joint-event is likely to have resulted in more policy-makers and non-academic stakeholders attending than would otherwise have happened.

The joint final conference was presented through a single website (the home page is shown in the figure below). This site advertised the joint event and gave details of the agenda, as well as practical information. It also provided a one-page introduction to each of the three projects, with links to their respective websites.

Figure 34: Website of the joint final DEMOSEC conference

Source: http://www.jointfinalevent2014.eu/

The fact that the conference was a joint effort was reflected in its structure, with all three projects contributing equally to all parts of the two-day event. Representatives of each project participated as speakers, chairs and panel members in every session, allowing for a systematic exchange and discussion of the results from all three sources.

For conference attendees, this joint-event is likely to have provided a broader, more comprehensive view of the topic of surveillance than would have been possible at individual project events. Indeed, it may have persuaded some to attend at all.

The **joint policy brief** was discussed at the end of the conference, but was still in development at the time of writing, and due to be published later in 2015. It is likely to reach a wider audience than the final event, and it is hoped that it will help to inform future policy decisions and surveillance activities. However, the brief is likely to be a collation of separate contributions from the respective projects rather than an attempt to provide an integrated synthesis of knowledge in the field.

F.11.5 Issues and challenges encountered

The organisation of the main cluster activity – **the final joint event** – was felt by participants to be a challenge. They reported a lengthy process of negotiation between the three consortia to agree on dates, guest speakers and so on, which required significantly more work than

organising a conference for one project alone. It was not clear to the partners whether this additional cost and effort was justified by the additional value gained from hosting an event together.

One explanation given for the difficulties experienced was that the three projects had different 'styles' and worked according to their 'own logic' and internal decision rules. For example, the RESPECT project required all project partners within its consortium to agree to any decisions, which made the negotiations between it and the other projects more complicated and drawn out. This challenge was overcome by persistence but no 'solution' was found that would make it easier next time.

The different consortia also came from different conceptual and theoretical starting points, focussing on technological, legal and sociological aspects respectively. While this offered the opportunity for fruitful collaboration, it also required more time to reconcile the different backgrounds and approaches.

More generally, the **project coordinators** were the ones most directly involved with the other projects in the cluster, both through the initial Commission meeting and subsequent exchanges between the projects. By comparison, there was limited direct interaction amongst other participants in the different projects, except (and until) the organisation of the final joint conference. It would appear that some project partners may have been open to closer cross-project collaboration, and therefore frustrated by their limited and late involvement in cooperative activities. For some, the clustering initiative does not appear to have particularly influenced the way the projects planned and carried out their research, and they expressed disappointment at the absence of any 'real' research collaboration, or at least efforts to ensure coherence and cross-learning between the three projects.

Possibly, the top-down nature of the collaboration – initiated by the Commission and focussed on interaction between project coordinators - meant that other project members were unable to identify and initiate potential collaboration opportunities, where these would have been beneficial. At least one partner is known to have had ideas for additional cross-project collaboration that were not taken up by the project, possibly reflecting a desire to focus on one's own project rather than the opportunities afforded by the cluster (that may have required additional effort).

Project participants also pointed towards challenges related to the **EU grant process**, and expressed frustration with a lack of flexibility that made it difficult to accommodate cross-project collaborative activities.

They highlighted that the strict requirements to deliver predefined work packages and outcomes, as defined in the Description of Work, makes it difficult to take advantage of opportunities that emerge as a result of interaction with other projects. Also, some found it difficult to engage the Commission on issues beyond the formalities of the contracts, and believed that the possibility of more dialogue with the project officers would help find room to accommodate reasonable adjustments needed for the collaboration to advance. Some also mentioned that changes to the project officers assigned during the projects also did not help in this context.

F.11.6 Conclusions and lessons learnt

The launch of the cluster initiative relied on the awareness shown by the responsible Commission Services that similar topics were addressed by different parts of FP7. They were able to identify the complementarity between the separate actions at an early stage and coordinate the calls for proposals. The joint call seems to have been appropriate and sensible, and worked well.

The experience also shows that clustering projects can achieve **positive results**. The joint conference, in particular, was perceived positively by the project participants involved and is likely to have resulted in greater visibility for the projects and their results than would otherwise have been achieved (although it is not clear that this outweighed the additional costs incurred in coordinating such an event).

There is also some (limited) evidence of **cross-learning between the projects**, with greater awareness of the activities of the other projects, and some efforts to build on and take account of

others' work and results during the course of the research. These benefits were achieved with 'light touch' encouragement by the Commission and at no additional cost to the programme. However, overall, cross-project collaborative activities remained a marginal aspect of the projects, and the benefits and impacts of the cluster were quite limited as a result.

It has been suggested by project representatives that the cluster idea was introduced too late in the project planning process for cooperation to be embedded meaningfully into the respective research plans. However, it was also noted that even with earlier warning, the detailed planning of joint activities could not have taken place until the individual projects that would form the cluster had been selected.

There was also a **lack of clarity as to the scope and purpose** of the initiative, with a lack of communication between the EC and project coordinators, and between the coordinators and the wider project teams. The projects involved (through their coordinators) do not seem to have bought-in fully to the cluster idea, and tended to see the collaboration as a top-down additional requirement, rather than an opportunity to devote significant efforts to exploiting.

It is not clear, though, whether this means that the cluster fell short of expectations. This was a first attempt at creating a simple project cluster within the Security Research Programme, and the projects did indeed fulfil the specific requirements in terms of joint activities. However, some of the project partners had expected greater cross-project collaboration, and there was also some expectation on the Commission side to see the project coordinators use the initiative as a platform to further develop research collaboration beyond the minimum requirements set out by the Commission.

As the initiative was also intended to inform the Commission's thinking about future approaches, the case suggests the following **ideas** should be considered:

- The cluster could have been **more explicitly introduced**, and at an earlier stage – such that consortia could better understand expectations at the proposal stage, and better embed collaborative activities within project planning. However, it was noted that detailed planning of joint activities could still only take place once the individual projects that would form the cluster had been selected.
- The intended **scope and objectives** of the cluster could have been more explicitly explained. Several project partners expressed frustration that they were asked to collaborate without fully understanding why, or what the intended scope of the cooperation was. If the main aim was to enhance the dissemination of results, then making this clearer may have helped reduce confusion and frustration amongst those partners keen to develop more extensive collaboration between projects.
- **Project coordinators** have a key role in driving the cluster initiative. To a large extent, the results of the initiative hinge on the willingness of the coordinators to take ownership and drive it, and to bring the wider consortia into the process.
- If the clustering approach is to achieve more substantial research collaboration, this would probably require **adjustments**. Among the suggestions made by project representatives were: (i) to identify and focus efforts on specific topics of shared interest and not try to collaborate on everything covered by the various projects. On those topics, organising work packages or targeted events would ensure genuine collaboration; and (ii) to provide additional funding earmarked for collaboration, similar to network funding to cover transaction costs used in other areas. Collaboration takes time and resources, and projects are reluctant to engage if it means reallocating resources away from already planned research activities.
- Finally, clusters should be encouraged **to clearly present themselves** as a joint entity, making clear their strong cohesion and inter-working. The three projects investigated here formed the DEMOSEC cluster platform, but could have gone further by developing a joint project website (building on the joint event website).

F.12 Participation of smaller EU countries in FP7 Security Research Actions

The aim of **this case study** is to investigate the participation of smaller EU countries in the FP7 Security Research Programme. It explores overall participation patterns at the programme level, before focusing on four countries that have achieved relatively high participation rates. It explores the reasons for these participation levels, as well as the outlook for future involvement in European Security Research. The case study contributes to the evaluation of Security Research programme's attractiveness to actors in smaller Member States and its complementarity with other initiatives.

The case begins with short introduction, followed by an analysis of the participation of Member States in the FP7 Security Research Programme, in both absolute terms and in relation to their size, and then focuses on four examples of smaller countries that have achieved a relatively high participation rate: Luxembourg, Slovakia, Latvia and Estonia. Finally, the case draws conclusions and lessons and provides a series of suggestions for consideration for the future.

The research carried out for this case study includes desk research, analysis of CORDA data, and five interviews with representatives of NCPs and policy officers from the European Commission.

F.12.1 Introduction

The starting point for the analysis is the observation that many smaller countries have a relatively **high participation rate** in the FP7 Security Research Actions. This raises questions about the 'evenness' of participation across countries, the possible reasons for this, and indeed whether it matters.

The EU Framework Programmes are Europe-wide and it is recognised that **broad participation from the Member States** is an important concern. The standard requirement of having three different countries represented in each project is testament to this. The European Research Area (ERA) is meant to connect research systems across Europe and in the 2012 ERA Communication[195] it is made clear that the ERA should bring benefits to *all* Member States.

However, there are still **significant internal disparities** in terms of research and innovation performance in the European Union (also identified in the Innovation Union Scoreboard), further aggravated by the continuing financial crisis, and resulting in adverse effects on public research and innovation budgets[196]. In this context, Horizon 2020 now offers specific support to 'low-performing countries' and this includes, among other things, funding for transnational networks of National Contact Points (NCP).

The Commission[197] offers the following **possible explanations** for why participation rates may vary between countries:

- National level investment in research;
- Interaction and synergies between the FP and the national research system;
- Experience with FP procedures within national systems;
- Wage levels - variation in wages, even taking into account the variations in purchasing power (has a particularly strong impact on Marie-Curie Actions);
- Access to networks;
- Size of projects - large projects can be problematic for small and new actors;
- Information, communication, training and availability of advice.

[195] COM(2012) 392.

[196] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/spreading-excellence-and-widening-participation

[197] European Commission (2013): Factsheet: Spreading Excellence and Widening Participation.

This case study looks at whether smaller Member States have particular advantages or disadvantages with respect to participating in the Framework Programmes – and in the FP7 Security Research Programme in particular. It also considers whether there are initiatives and activities within certain countries that might offer useful learning or good practice for others, large or small.

F.12.2 Analysis of data on country-level participation and funding

Absolute levels of participation and funding

The *average* FP7 Security research project had 12 participants, and involved organisations from seven different countries. In fact, the Programme involved organisations from 48 different countries overall, including all 28 of the EU Member States (MS).

While on average each MS participated 121 times in the Security Research Programme and received €41m in EC contributions, as one might expect the actual levels of participation and funding varied widely – from just 9 participations and €1m in EC contributions for Malta, to 430 participations and €152m in EC contributions for the UK.

The number of participations and total EC contributions to each MS is shown in the table below. The table is sorted in descending order of EC contributions, and shows Germany, the UK, France, Italy and Spain to be the 'top' recipients of, and participants in the Programme (with €100m+ in funding and 300+ participations each).

Perhaps unsurprisingly, these top countries are also some of the biggest (population-wise), while those at the bottom of the table tend to be the countries with the smallest populations. To better visualise this, four groups of seven countries have been created, based on their population, and shaded differently in the table from the smallest (<4m, white) to the largest (>17m, dark grey).

Table 54: FP7 Security Research Programme participation and funding, by MS

Country	Total Population (m)	Total Participations	Total EC Contribution
Germany	81.8	380	159,862,017
United Kingdom	62.5	430	152,305,365
France	64.7	379	151,541,607
Italy	59.2	385	121,772,196
Spain	46.5	319	110,920,970
Netherlands	16.6	240	79,123,262
Sweden	9.3	144	62,294,867
Belgium	10.8	168	52,099,167
Austria	8.4	123	44,060,629
Greece	11.2	150	43,776,916
Poland	38.0	102	33,178,421
Finland	5.4	97	31,869,588
Ireland	4.5	79	26,075,799
Portugal	10.6	84	21,651,038
Denmark	5.5	41	14,257,242
Slovakia	5.4	25	7,125,091
Czech Republic	10.5	34	5,789,696
Luxembourg	0.5	19	5,033,438
Slovenia	2.0	25	4,457,149
Romania	20.3	38	4,351,272
Cyprus	0.8	15	4,162,720
Estonia	1.3	21	3,686,642
Hungary	10.0	27	3,536,682
Croatia	4.3	13	3,497,820
Bulgaria	7.4	21	2,321,091
Latvia	2.1	14	1,542,817
Lithuania	3.1	12	1,204,977
Malta	0.4	9	1,114,228
EU Total	**503.2**	**3,394**	**1,152,612,707**
Non-EU Countries		**347**	**110,875,337**
ALL COUNTRIES		**3,741**	**1,263,488,044**

Source: Technopolis analysis of CORDA data, December 2014

Relative levels of participation and funding

Despite the tendency of smaller countries to participate less in the Security Research Programme (and to receive less in total EC contributions) than larger countries in absolute terms, many are in fact participating at above average rates relative to their size.

In an attempt to take account of the size of different countries, the participation numbers and total EC contributions can be weighted by other factors, such as population, GDP or the number of researchers in the country. Based on these *relative* measures, the 'top' participating countries are different from those shown using *absolute* figures, and often include smaller EU countries.

For example, the table below shows the top 5 participating countries according to their number of participations per million population. These five all fall into the two smaller groups of countries, based on population size, and have between 17 and 38 participations per million population each. This compares with an overall rate of 7 participations per million population for the whole of the EU. For these five countries, the rate of EC contributions per member of population is also above average.

Table 55: Participations (and funding) relative to population size, top 5 countries

Country	Total Part's	Total EC contr. (€m)	Total population	Participations per 1m population	EC Contr. per pop. member (€)
Luxembourg	19	5.0	502,066	37.8	10.0
Malta	9	1.1	414,027	21.7	2.7
Cyprus	15	4.2	819,140	18.3	5.1
Finland	97	31.9	5,351,427	18.1	6.0
Ireland	79	26.1	4,549,428	17.4	5.7
…					
EU Total	**3,394**	**1,152.6**	**503,234,841**	**6.7**	**2.3**

Source: Technopolis analysis of CORDA data, December 2014

Similarly, based on the number of participations per €10bn of GDP, all but-one of the top 10 participating countries (Greece) have a population of <8m people. The 'top' 5 participating countries by this measure are shown below. These all fall within the smallest group of countries based on population, all with 7-15 participations per €10bn, compared with an overall EU rate of less than 3. For four of these countries, the rate of EC contributions (€) per €1m of GDP is above the EU average, the one exception being Latvia, where the rate is similar to the average.

Table 56: Participations (and funding) relative to GDP, top 5 countries

Country	Total Part's	Total EC contr. (€m)	Total GDP (€m)	Participations per €10bn GDP	EC Contr. (€) per €1m GDP
Estonia	21	3.7	14,709	14.3	251
Malta	9	1.1	6,600	13.64	169
Cyprus	15	4.1	19,062	7.9	218
Latvia	14	1.5	18,015	7.8	86
Slovenia	25	4.5	36,220	6.9	123
…					
EU Total	**3,394**	**1,152.6**	**12,789,849**	**2.7**	**90**

Source: Technopolis analysis of CORDA and OECD data

Finally, the top five participating countries according to the number of participations per thousand FTE researchers are shown below. Each has 5 or more participations per 1,000 FTE researchers, compared with an overall EU rate of 2, as well as a rate of EC contributions per FTE researcher that is above the EU average. Each country has a population of less than 5m people.

Table 57: Participations (and funding) relative to researcher population, top 5

Country	Total Part's	Total EC contr. (€m)	Total FTE Researchers	Part's per 1,000 FTE Researchers	EC Contr. per FTE Researcher
Cyprus	15	4.2	905	16.6	4,600
Malta	9	1.1	599	15.0	1,860
Luxembourg	19	5.0	2,636	7.2	1,910
Ireland	79	26.1	14,176	5.6	1,839
Estonia	21	3.7	4,077	5.2	904
…					
EU TOTAL	**3,231**	**1,152.6**	**1,570,616**	**2.1**	**734**

Source: FTE researcher figures for 2010, taken from Eurostat

According to these relative measures, therefore, it appears that many small countries are punching above their weight in the FP7 Security Research Programme. However, it may be that this is not specific to the Security Research area, and that a similar picture exists across the Framework Programme. To test this, a country's level of participation in the Security Research Programme can be compared with its participation in the wider Cooperation Specific Programme.

The Security Research Programme is one of the smallest themes of the Cooperation Specific Programme, and on average (across all EU countries) it accounts for just 4.4% of all participations. However, for some countries it is much more significant. For example (as shown in the final column of the table below), Luxembourg, Malta and Slovakia all have rates of Security Research theme participation (relative to the wider Cooperation Specific Programme) that are at least double the average.

Table 58: Participation in the FP7 Security Research Programme and the Cooperation Specific Programme

Country	Total Participations (Security)	Total Participations (Cooperation)	Security participations as % of Cooperation
Luxembourg	19	173	11.0%
Malta	9	86	10.5%
Slovakia	25	282	8.9%
Latvia	14	167	8.4%
Estonia	21	276	7.6%
Poland	102	1,345	7.6%
Cyprus	15	223	6.7%
Ireland	79	1,188	6.6%
Greece	150	2,464	6.1%
Romania	38	644	5.9%
Croatia	13	224	5.8%
Portugal	84	1,467	5.7%
Bulgaria	21	367	5.7%
Lithuania	12	214	5.6%
Finland	97	1,883	5.2%
Austria	123	2,487	4.9%
Sweden	144	3,058	4.7%
Italy	385	8,297	4.6%
Spain	319	6,953	4.6%
France	379	8,341	4.5%
United Kingdom	430	9,786	4.4%
Netherlands	240	5,536	4.3%
Belgium	168	3,926	4.3%
Slovenia	25	605	4.1%
Czech Republic	34	876	3.9%
Hungary	27	839	3.2%
Germany	380	12,872	3.0%
Denmark	41	1,799	2.3%
EU TOTAL	3,394	76,378	4.4%

Together with the previous analyses, this suggests that not only are many of the smaller EU countries 'heavy participants' (and funding recipients) compared to their size, but also that at least some of this effect is specific to the FP7 Security Research theme, and not reflected in the Cooperation Specific Programme more widely.

In the next sections the participation of a selection of four smaller EU countries is explored in more detail. Each focus country has a high level of participation in the Security Research Programme relative to their population, GDP, research base and / or their level of participation in the Cooperation Specific Programme overall.

F.12.3 Exploration of selected countries - Luxembourg

Participation in the FP7 Security Research Programme

Luxembourg's relative level of participation in the FP7 Security Research Programme has been above the EU average according to all measures, as show in the table below.

Table 59: Luxembourg – measures of participation levels

Country	Pop.	SEC Part's...	...per 1m Pop.	... per €10bn GDP	... per 1,000 FTE researchers	... as % of Cooperation participations
Luxembourg	0.5m	19	38	5	7	11%
EU total	**503m**	**3,394**	**7**	**3**	**2**	**4%**

Source: Technopolis analysis of CORDA data, December 2014

The country's relative rate of EC contributions is also above the EU average across all measures (table below). Contributions per population member are particularly high.

Table 60: Luxembourg – EC contributions

Country	EC funding (€m)...	... per popul. member (€)	... per €1m GDP (€)	... per FTE researcher (€)
Luxembourg	5.0	10.0	128	1,909
EU total	**1,153**	**2.3**	**90**	**734**

Source: Technopolis analysis of CORDA data, December 2014

Looking at the characteristics of the participating organisations, Luxembourg is similar to most of the other countries studied here with about 61% of EU funding going to Private for Profit Organisations (excluding education) (PRC) and 22% to Higher or Secondary Education Organisations (HES). Two organisations, the software company Intrasoft and the Interdisciplinary Centre for Security, Reliability and Trust (SnT), a research centre under the University of Luxembourg [198], accounted for more than half of the €5m in EC contributions awarded to participants in Luxembourg.

National strategy and policy

Security research is a high priority in Luxemburg. The issue is primarily driven by the ICT and banking industries, with a particular focus on digital infrastructure and security.

The Ministry of Economy has also been a driver, putting significant emphasis on these issues. The Ministry of Research sets goals for, for example, SME involvement in FP7 and Horizon 2020.

The NCPs are attempting to show potential participants the benefits of 'the EU route', such as access to research and innovation knowledge. They can play a coordinating role to get people together and provide customised opportunities to SMEs and others. The FP7 NCPs are affiliated with Luxinnovation, the national agency for innovation and research, and this allows them to coordinate with colleagues managing national funding, and use the organisation's network to engage with stakeholders.

Domestically, the Ministry of Research funds security research. The government has also launched the Luxembourg Cluster Initiative[199] with six themes that are similar to the FP7 themes.

Specific programmes to encourage participation in EU research programmes have been set up for FP7 ('Fit for Europe') and for H2020 ('Fit4Horizon2020').[200] Under H2020, the programme is particularly aimed at SMEs and offers €5,000-10,000 to pay a consultant to help with proposal preparation.

How to explain participation

The government pushing ICT and security research is one factor driving Luxembourg's participation. It was also reported that, being a small country, it is easier for NCPs to get access to government and NCP networks. The country's focus on applied, as opposed to basic, research also fits well with the EU programmes.

[198] Université de Luxembourg (2015) SnT – Interdisciplinary Centre for Security, Reliability and Trust.

[199] Luxinnovation (2015) Luxembourg Cluster Initiative.

[200] Luxinnovation (2015) Fit4Horizon2020.

Another major factor has been the facilitating role of Intrasoft and SnT, the two most frequent participants from Luxembourg. They have helped to bridge the gap to other partners and bring collaborators from national projects into EU projects. Reportedly, SnT was particularly instrumental in bringing end-users into projects.

Good practice

Several aspects of Luxembourg's approach to FP7 Security Research were reported to have worked well. First, the position of the NCPs within the innovation agency helped them to coordinate and facilitate access to their target audience.

Secondly, the importance for NCPs of 'customising' and 'targeting' the approach to each individual client was emphasised. This involves doing background research, targeting those companies that are interested in EU programmes and preparing a pitch that will appeal to them.

Benefits from participation

The main benefits from involvement are reported as including helping companies to stay competitive and maintaining networks. So far, the main 'selling point' of the Framework Programme in Luxembourg has been networking. The FP is a good opportunity to filter partners for future collaboration, not only within the EU but beyond Europe as well. This can create lasting relationships, for example between large multinationals and SMEs.

It is too early to say whether the outputs from the projects themselves will be useful. The Security ICT sector evolves very quickly and, in some cases, the outputs can be out of date before the projects are completed. For this reason, the direct project outputs should not be the only aim.

Future potential

There is still thought to be the potential for a better level of participation in H2020 from Luxembourg. SnT and Intrasoft understand the processes well and are expected to continue to participate. Indications are that others who were active in FP7 are also going to be equally active in H2020.

The next 'targets' for NCPs are those organisations that have been less engaged. There are still many organisations with the 'right profile' that do not know about the Framework Programmes.

Barriers to participation

As a small country, Luxembourg needs to prioritise and cannot participate in everything.

One of the main challenges is to convince research organisations and companies that it is worthwhile applying. National funding is often preferred by research organisations, as it is less competitive and more flexible (thematically open). There is also a perception that EU funding is difficult to manage.

F.12.4 Exploration of selected countries - Slovakia

Participation in the FP7 Security Research Programme

As shown in the following table, Slovakia's rate of participation in the Security Research Programme is similar to the EU average relative to population and GDP. However, since Slovakia's participation in the Cooperation Specific Programme overall is relatively low, the Security Research theme takes up a much higher share (9%) of its participation than for other countries. In other words, Slovakia has been relatively successful in the Security Research Programme compared to other Cooperation Specific Programme themes.

Table 61: Slovakia – measures of participation levels

Country	Pop.	SEC Part's…	…per 1m Pop.	… per €10bn GDP	… per 1,000 FTE researchers	… as % of Cooperation participations
Slovakia	5.4m	25	5	4	2	9%
EU total	**503m**	**3,394**	**7**	**3**	**2**	**4%**

Source: Technopolis analysis of CORDA data, December 2014

The rate of EC contributions received by Slovakia is below the EU average when compared with population or the number of FTE researchers, but is slightly above average relative to GDP (table below).

Table 62: Slovakia – EC contributions

Country	EC funding (€m)...	... per popul. member (€)	... per €1m GDP (€)	... per FTE researcher (€)
Slovakia	7.1	1.3	106	469
EU total	**1,153**	**2.3**	**90**	**734**

Source: Technopolis analysis of CORDA data, December 2014

PRCs received 71% of Slovakia's funding from the Security Research Programme. The most successful among them was Ardaco, working in the areas of ICT and security. The company received funding for 3 projects under the Security Research theme. Ardaco itself received 50% - and the three projects (including other Slovak partners) accounted for 80% - of all funding for Slovakia from the Security Research Programme.

The University of Zilina participated in four FP7 projects. Public end-users (e.g. Ministries and Police) did not participate extensively. Five higher education institutions received a combined 24% of Slovak FP7 Security Research Programme funding.

National strategy and policy

There is no national strategy to strengthen participation in the Security Research Programme. Reportedly, there were initiatives to pursue this issue with the Ministry of the Interior throughout the preparatory action, FP7 and H2020, but apparently, there has been limited interest from the government. There is no national programme for security research. There were however, general funding schemes to support participation to FP7 (see below).

There were changes concerning the Security NCP over the FP7 period. Between 2011 and 2013, there was a 'common approach', which led to the organisation of infodays and a workshop with FP7 proposal evaluators (who shared information and knowledge with participants).

Reportedly, more attention has been paid to distributing information in the media about the FP7 Security Research Programme than has been the case for other FP7 themes. The NCP is trying to push Slovak researchers to attend meetings and participate at brokerage and networking events, conferences and other events connected with security and trying to engage interested (private) organisations.

Two specific funding schemes were available to support participation in FP7:

- The Slovak Research and Development Agency (SRDA) supported preparation of proposals in the period 2007-2010 with an annual budget of €665k. Funding was available to cover salaries and travel costs incurred in proposal development. The amount available depended on the applicant's role in the project and ranged from €5k to €17k.
- A co-financing scheme for FP7-funded projects, providing 25% of research costs for Public Bodies (excluding research and education) (PUB) – topping up the 75% of costs covered by EU funding in collaborative projects. All applications to the scheme have been granted so far.

In addition, universities could receive match funding from the Slovak government, according to a funding formula that is revised annually. The scheme has been in operation for several years, but it is unclear whether it will continue in the future.

How to explain participation

Ardaco drove Slovak participation. The company accounted for almost half of the FP7 funding obtained and facilitated an even higher share through their involvement. Ardaco first got involved in FP7 through (self-funded) participation in a European Technology Platform (ETP). From there, they took advantage of support from the NCP and funding from the SRDA to apply for FP7 funding.

FP7 industry partners in Slovakia all know each other and many of them are related to Ardaco. New companies have been formed by people formerly involved with Ardaco, such as G.A. Drilling and ADDSEN.

Good practice

The organisational setup of the NCP changed several times during the FP7 period, and some features under the different models were reported to have been beneficial. For instance, selecting the NCP host institution by public procurement appears to have given the right financial incentives.

One event that was reported to have been particularly useful was a workshop with FP7 proposal evaluators, which gave Slovak would-be applicants a very good understanding of what was required in an FP7 application.

The success of the company Ardaco also provides elements of good practice: Guided by the NCP, they used the ETP as a stepping-stone to learn about FP7 before engaging fully in project applications. This kind of light-touch entrance point may be useful to companies who have reservations about participating in EU programmes.

Benefits

The benefits from participating in the FP7 Security Research Programme are not all about money. The opportunity to cooperate with the most important players in Europe is attractive, as is the prospect for SMEs to develop new projects. Correspondents also emphasised the *prestige* associated with participating in an FP7 project.

Future potential

The Slovak NCP for security research has published a series of recommendations on how to increase Slovakia's participation in H2020[201]. This recommends some measures to support H2020 participation directly – for example a new version of the SRDA scheme from FP7 – and argues that more fundamental changes to the Slovak R&I system are necessary.

Barriers

There is no national programme for security research, which interview partners believe is detrimental to Slovak participation. Public support to R&D in the Slovak Republic has increased significantly (EUR 86 million in 2000 to EUR 219 million in 2010), notably due to the financing from EU resources (mainly through Structural Funds)[202].. However, in general, correspondents argued that the government ought to be more active in encouraging R&D through tax credits or other means.

Public sector end-users have not participated as much as they could have. They are focussed on fulfilling their primary obligations and have difficulties finding resources to dedicate to FP7 research. For example, it can be difficult to hire someone specifically to work on a project.

There are few big companies in Slovakia, so the main potential for participation lies with SMEs. The first step is to find them in order to be able to engage with them. Convincing them to participate can be difficult, as they do not all have the same 'vision' as Ardaco. Also, many companies do not have the resources to prioritise long-term benefits of R&D over short term 'survival', while for others – such as software companies – their innovation cycle is too short for FP7 to be relevant.

F.12.5 Exploration of selected countries - Latvia

Participation in the FP7 Security Research Programme

Latvia's participation in the FP7 Security Research Programme is high relative to GDP and the number of researchers in the country. The Security Research Programme also accounts for a

[201] Scope III/2014 eNEWSLETTER o 7. rámcovom programe EÚ (Slovak FP7 newsletter), pp. 8-9.

[202] Deloitte (2013) Researchers' Report 2013. Country Profile Slovak Republic.

much higher share of FP7 participations in Latvia than in other European countries (see table below).

Table 63: Latvia – measures of participation levels

Country	Pop.	SEC Part's...	...per 1m Pop.	... per €10bn GDP	... per 1,000 FTE researchers	... as % of Cooperation participations
Latvia	2.1m	14	7	8	4	8%
EU total	**503m**	**3,394**	**7**	**3**	**2**	**4%**

Source: Technopolis analysis of CORDA data, December 2014

Latvia's rate of EC contributions, meanwhile, is below the EU average across all measures. EC contributions relative to GDP are close to the EU average (table below).

Table 64: Latvia – EC contributions

Country	EC funding (€m)...	... per popul. member (€)	... per €1m GDP (€)	... per FTE researcher (€)
Latvia	1.5	0.7	86	396
EU total	**1,153**	**2.3**	**90**	**734**

Source: Technopolis analysis of CORDA data, December 2014

Unlike the other countries in this study, PRC organisations have played a relatively modest role in Latvian participation, accounting for only 21% of participations and 28% of funding received. Instead PUB participants – including the Ministry of the Interior and the Maritime Administration – have been much more active, receiving 29% of total funding compared to 0-6% in the three other countries.

National strategy and policy

In Latvia, there is no particular strategy for FP7 participation. Instead, the main effort made at the national level relates to promotion and information, and the NCP organises information days and undertakes other efforts to encourage participation.

There is no national funding programme for security research as such. A related field, 'safety', does have funding available but it does not have quite the same focus. There is no support available for preparing proposals, but the Government does cover the overhead costs not covered by FP7 grants.

How to explain participation

The high participation rate in Latvia is mainly due to interest from end-users, including national government institutions.

Good practice

The importance of 'success stories' was highlighted, in particular because it is difficult to obtain EU funding (the success rate in Latvia is 1:10), hence many actors do not have first-hand knowledge about how beneficial participating in a project can be.

The high participation rate for public end-users in Latvia is also remarkable, although there is no evidence of any particular initiative or programme to support this. In other countries it was reported that PUB organisations were difficult to engage, but Latvia provides an illustration that a high participation rate from this type of organisation can be achieved.

Benefits from participation

For ministries and other public sector bodies, participation in the Security Research Programme allows them to exchange about recent trends and future possibilities from counterparts in other countries.

Universities are reportedly 'always happy' to receive funding, and are primarily driven to participate by the funding available in their field of research. For industry, the funding tends to be less important, compared with the opportunity to learn about the wider context of the European market in their area. Large companies that were used to being the 'big players' at home reportedly benefitted from this kind of 'reality check'.

Future potential

The participation rate is not expected to change significantly in H2020 compared to FP7. Border guards and coastal guards have recently started to express an interest in the Security Research Programme, and higher participation can be expected from them. However, there is some concern about university participation, which may not be maintained at the current level. A study of Latvian participation in EU programmes is foreseen next year.

The aim is to increase the success rate for proposals rather than the number of applications. To achieve this, applicants will need be more aware of opportunities and better prepared, for example to join a project as a partner.

It was reported that more support was needed from the European Commission, for example in the form of a handbook for applicants and more frequent visits to the country to support the work of the NCP and to lend credibility in in eyes of stakeholders.

Barriers to participation

One significant barrier to participation is the very high oversubscription. It is felt to be easier for applicants in older Member States because they know the procedures well from previous programmes. As such, it is felt that more should be done from the Commission to support newer Member States in the practical aspects of the application process.

Reportedly, another barrier is the mind-set of Latvian would-be participants, who would not be used to working with very long time horizons and not be able to wait for several years for a call to appear in their particular field.

PUB participants have had difficulties with their participation due to internal administrative rules and regulations, for example about how to pay for additional work hours. Some agencies have had to drop out of projects. A change is needed to make future participation more seamless.

Finally, the availability of Structural Funds makes many actors 'less desperate' for funding and discourages them from applying for Framework Programme funding. Even if working with Structural Funds is more demanding in some aspects, applying for Framework Programme projects can be even more daunting as a first-time participant who doesn't know 'the rules of the game'.

F.12.6 Exploration of selected countries - Estonia

Participation in the FP7 Security Research Programme

Like the other countries in this study, Estonian participation is high relative to its size, as shown in the table below. The main groups of participating organisations are PRC (62% of funding) and HES organisations (22% of funding). Most of the companies involved are small (fewer than 100 employees) and many of these are owned by individuals with links to academia. There are no 'big players' driving Estonian participation.

Table 65: Estonia – measures of participation levels

Country	Pop.	SEC Part's...	...per 1m Pop.	... per €10bn GDP	... per 1,000 FTE researchers	... as % of Cooperation participations
Estonia	1.3m	21	16	14	5	8%
EU total	**503m**	**3,394**	**7**	**3**	**2**	**4%**

Source: Technopolis analysis of CORDA data, December 2014

Estonia's rate of EC contributions is above the EU average across all measures, and is particularly high relative to the country's GDP (table below).

Table 66: Estonia – EC contributions

Country	EC funding (€m)...	... per pop. member (€)	... per €1m GDP (€)	... per FTE researcher (€)
Estonia	3.7	2.8	251	904
EU total	**1,153**	**2.3**	**90**	**734**

Source: Technopolis analysis of CORDA data, December 2014

National strategy and policy

The Estonian government supported participation in FP7 generally, but not Security Research specifically. The national research strategy addresses FP7 participation, but it contains nothing specific about security research. Similarly, the national Defence Industry Policy, which covers R&D and manufacturing for defence, security and other related purposes, emphasises the importance of international collaboration, but does not mention the EU Framework Programmes specifically.

The Ministry of Defence does, however, offer small grants for national (Estonian) security research projects (~€300k spread across ~4 projects annually).

Overall though, security research has not been a political priority in Estonia and the high participation rate to FP7 is felt to have 'just happened'.

Instead, the drive to support FP participation has come mainly from the National Contact Points (NCPs). This has been helped by consistency in NCP staff over the past decade.

To encourage participation, Estonia also provides support for the preparation of proposals. The awards provided depend on the role the Estonian organisation is playing in the project (e.g. up to €3,600 for project coordinators and up to €1,200 for participants, provided they are at least WP leaders or similar).

How to explain participation

The small size of Estonia can make networking and interaction between necessary actors easier. For instance, there is a security team cluster and a security industry association, which gather all the main actors, including competence centres and businesses. They organise events together and other similar activities. They were not set up for the purpose of participating in Framework Programmes but they help increasing participation.

Good practice

Estonia has been able to keep a team of NCPs together over a period of time, which has allowed them to build up competence. This could be seen as good practice compared to other countries where frequent personnel change is reported to have created disruptions in the service provided to potential participations.

Also, NCPs have been able to take advantage of existing industry networks. This has facilitated access to a large group of stakeholders they might not otherwise have been able to reach effectively.

Benefits from participation

The most important benefits from participation are seen to be contacts and cooperation. Once you have your foot in the door, participation in one project will often lead to the next one. Also, for small companies who want to sell technology, projects can help to get to know potential buyers.

Money is not the most important factor driving participation, but it is still important. External funding allows companies to innovate when there is no room for R&D in the regular budget. For universities, the Estonian system provides very little institutional funding and FP7 provided an additional funding opportunity in a highly competitive national landscape.

Finally, there are certain issues – like border security – where collaboration has a clear European added value, and it is felt to be important for Estonian partners to be involved.

Future potential

Estonia does not have a specific strategy for European Security Research going forward. However, in FP7 there were no Estonian coordinators of Security research projects, and there is a desire to see this change in H2020.

Barriers

Estonia does not have a large security industry. Most calls require a large industry partner and, as a consequence, Estonian partners often end up as participants that are contributing to

develop technologies that others will use. It is felt that a few big associations dominate the sector and that it is difficult for Estonian companies to compete against them.

Estonian organisations typically find themselves better able to participate in smaller projects, but in H2020, the Commission is moving towards larger projects, such as Public-Private partnerships, which may make it difficult for small countries to participate.

F.12.7 Conclusions and lessons learnt

This section brings together the findings from the four example countries, drawing out any similarities and differences in participation patterns and the reasons behind this, as well identifying the main benefits to participation for small countries, possible good practice examples, prospects for the future and suggestions for improvement.

Explaining participation

Different avenues were explored to explain the high levels of participation in different countries. The main factors reported were:

- **The existence of national strategies and programmes for security research:** In Luxembourg, security research is a clear national priority driven by the banking and ICT sectors and taken up by the government. Luxembourg was also the only country to report the existence of significant and specific national funding for security research, while Estonia also has a limited amount of funding available for security research through the Ministry of Defence. This correlates with data from CORDA, which shows that Luxembourg has the highest relative participation rate, followed by Estonia.
- **Leading actors driving national participation:** In Luxembourg participation was driven by the company Intrasoft and the university research centre SnT, while in Slovakia the ICT and security company Ardaco contributed significantly to national participation. In both cases, it was reported that these lead actors were able to facilitate the participation of other national actors. In Latvia, PUB participation was reported as the main explanation of the high participation rate. The type of dynamic described here is probably unique to smaller countries were a few actors can have a proportionately big impact.
- **In smaller countries it is reported that 'everyone knows each other':** While this is a slight exaggeration, the relatively small populations and geographical proximity can make it easier to access relevant stakeholders and government actors. Variations of this explanation were reported for Estonia, Slovakia and Luxembourg. In Estonia, existing industry networks were accessed by the NCP, whereas Luxembourg reported that it was easy to access government actors. In Slovakia, it was reported that networks of companies were more informal (centred around Ardaco) – although it was also reported that interest from the government was limited.
- **Specific support matters:** In Slovakia in particular, the NCP had played a very active role, and the specific funding available to support preparation of proposals had been taken up by key actors.

Examples of good practice

Correspondents in the four countries gave several examples of good practice that had helped them be effective in their role as NCPs. These included:

- **Organisation of NCPs:** Several organisational aspects in the setup of NCPs were emphasised: In Estonia, a stable team of NCPs had managed to build up expertise over several years, which helped them be effective. In Luxembourg, it was reported that the NCPs affiliation with the R&I agency Luxinnovation had facilitated access to government and stakeholders alike. Finally, in Slovakia, choosing the NCP host institution through public procurement appears to have helped provide incentives.
- **Taking advantage of existing networks to engage with stakeholders:** In Estonia, these were industry networks that were set up for different purposes but that also provided an effective channel for the NCP to relevant stakeholders. In Luxembourg, the affiliation of

the NCP with Luxinnovation had a similar effect, enabling easy access to the research and business communities already funded through national programmes.

- **'Customised' engagement with SMEs:** All countries reported that it could be difficult to engage with SMEs, which may not see EU programmes as relevant to them. In Luxembourg, it was seen as particularly important to do background research on potential clients and to tailor an offer that fits their needs. Another approach to engaging with SMEs was found in Slovakia: here, the leading FP7 participant Ardaco had, used a European Technology Platform (ETP) as a stepping stone towards full participation in FP7 projects. Gradually building experience and confidence with the EU processes can be important to companies to overcome reluctance to participate.
- **Relevant information for new applicants:** The Slovakian NCP reported that an event organised with presentations from FP7 proposal evaluators had been particularly helpful to applicants because it provided an insight into the evaluation process that newcomers lack. Another important source of information could be 'success stories' from successful applicants to showcase the potential benefits of applying and to encourage potential applicants to invest the time and effort to try.

Benefits from participating

There was relative consensus in the four countries about the main benefits of participating. There was general agreement that getting funding was important, but also that there were other, often more important, drivers:

- **Networking**: This was a 'main selling point'. Networking is seen as important for providing knowledge about new developments that helps organisations to stay up to date and competitive. It is also important for establishing relationships with potential collaborators or business partners.
- **Collaborating on shared problems**: For PUB organisations, there was a clear European Added Value in collaborating on issues like border control.
- **Additional funding gives room for innovation**: SMEs in particular often have difficulties setting resources aside for R&D with long-term benefits but without short-term returns. Funding from the FP7 Security Research Programme can allow some SMEs to do that.
- **Project outputs**: Correspondents were cautious about over-selling the benefits of specific project outputs. It is still too early to say, but considering the relatively long programming process, there is always a risk that rapid technological evolution could limit their usefulness.

Future prospects for participation and challenges faced

It was largely expected that participation levels in Horizon 2020 Security Research would be similar to that seen during FP7. There was, however, a set of commonly agreed barriers that still persist:

- **Convincing stakeholders to participate**: In newer Member States, this problem was particularly related to the fact that many actors lack experience with FP projects and shy away from investing time and effort. More generally, the availability of alternative sources of funding (national programmes or Structural Funds) that might be less competitive or more familiar can act as a deterrent. In addition, SMEs often do not have the resources available to invest in R&D and are reluctant to engage in long-term projects.
- **Small countries are disadvantaged in large projects:** Large projects tend to be lead by big European players, often from large Member States. To the extent that smaller Member States participate, it tends to be in minor roles with less benefit to the participant. There were concerns voiced about the direction being taken in H2020, with more large public-private partnerships, which tend to favour organisations with good connections, and may exclude small organisations from new Member States.
- **Engaging public sector end-users:** In three of the four countries assessed, participation from public sector end-users was relatively low. Even in Latvia, the only country where with

a relatively high PUB participation rate, it was reported that administrative rules and regulations had been an obstacle for effective participation by this group and forced several partners to drop out.

Suggestions for future improvement

The findings of this case study point towards actions that could be made at national and European level to strengthen the participation of smaller Member States in Horizon 2020 and future security research programmes:

- **Others can learn from smaller countries:** One of the key strengths identified across the four countries has been the effective internal coordination. In some cases this was informal, but there were also several examples of how the support system was effectively set up to exploit existing networks to ease access to stakeholders. Even larger Member States could draw inspiration from these examples to improve their national systems.
- **European funding instruments should accommodate SMEs**: The countries studied here all reported that SMEs were their most important constituency, and expressed frustration over the barriers they saw for them to participate effectively in European projects. In particular, concerns were raised about the tendency towards larger projects and consortia.
- **Additional support for newer Member States:** Many newer Member States are comparably small and it was suggested that additional support from the Commission in the form of practical guidance (e.g. a 'handbook') and more frequent visits to these countries might help NCPs be more effective. In these countries, many organisations are relatively inexperienced and the national support systems are limited in scale and scope.
- **Reform of public sector rules to allow FP participation:** Several countries reported that PUB organisations that could benefit from participating were constrained by internal rules and regulations. Reforms will be needed to facilitate future participation from this important group of end-users.

F.13 Dealing with challenges in diverse project settings involving numerous types of partners

This case study considers the difficulties involved in managing research projects with partners from diverse backgrounds, and explores examples of these challenges, as well as the approaches taken to address them within specific FP7 Security projects. Specifically, it investigates three projects that involved various types of partners.

Drawing on testimonies from project coordinators and participants, the case considers the challenges that have been faced in managing partners from diverse professional and disciplinary backgrounds and identifies (successful) approaches to addressing the challenges and issues faced. The case then draws conclusions and lessons learned for H2020.

The work is based on extensive desk research and interviews conducted with project participants and experts in the field of security research.

F.13.1 Introduction

The difficulties project coordinators face in dealing with large and **diverse collaborative research teams** has been much considered in academic and grey literature, and many researchers have investigated the organisational, cultural, national or functional challenges of collaboration across boundaries. A number of important recent studies, which focus on interdisciplinary scientific and technical work, have identified challenges of managing research teams and large EU sponsored research actions. For example, the management literature highlights the importance of an appropriate management of the team in settings where tasks are undertaken by diverse groups, and that research management needs to be undertaken at the very start of any work.

- In a study of a large EU-funded project Ettore[203] (2000) addresses the misconception that many researchers suppose that good research management is acquired through a process of trial and error and demands little thought, skill or training. As illustrated in the cases below, emphasis on the intense and **professional management** of large diverse research teams is essential to ensure positive outcomes. For Ettore successful, high-quality research is a resource that "*demands sensitivity to diversity*" and "*an awareness of group processes*" in a scientific context.
- The challenges for project managers include effective research management, which requires **close collaboration of researchers**, sometimes specialised in different scientific areas and residing in various locations. According to Zikos et al (2012) "*Successful research management requirements include equal teamwork and efficient coordination, in order to increase the impact of the research outcomes and provide added value knowledge*."[204]
- The emphasis on **managing differences and creating synergy** through effective management has grown, with Lee et al. (2015) noting that research collaboration depends not upon individuals but upon teams, and collaboration between them[205] – a finding that supports earlier work on this topic by Pei and Porter (2011)[206]. A Security Research project consortium includes not only the research partners, and for De Rosa et al. (1999)[207] effective research management requires all partners' active participation, including communities, interest groups, stakeholders and policymakers.

[203] Ettorre, E. (2000) Recognizing diversity and group processes in international, collaborative research work: A case study. *Social Policy & Administration,* 34(4), 392-407.
[204] Zikos, D., Diomidous, M., Mantas, J. (2012) Challenges in the Successful Research Management of a Collaborative EU Project, Acta Inform Med. 2012 Mar; 20(1): 15–1.
[205] Lee, Y. N., J. P. Walsh and J. Wang (2015) Creativity in scientific teams: Unpacking novelty and impact. *Research Policy* 44(3): 684-697.
[206] Pei, R. M. and A. L. Porter (2011) Profiling leading scientists in nanobiomedical science: interdisciplinarity and potential leading indicators of research directions. *R & D Management* 41(3), 288-306.
[207] De Rosa CT, Rosemond ZA, Cibulas W, Gilman AP (1999) Research management in the Great Lakes and St. Lawrence River basins: challenges and opportunities *Environmental Research,* 80(3), 274-9.

The challenges identified above are all directly relevant to the projects of the FP7 **Security Research Programme that** involve not only participants from different disciplinary backgrounds, but also bring together experts from research, industry and end-user organisations including civil society organisations. On average, FP7 Security Research projects involved twelve different participating organisations, which is slightly above the Cooperation Programme average of eleven. Most also involved participants from three (45%) or all four (42%) of the main types of organisations (HES, PRC, PUB and REC), while just 11% involved just two types, and 2% only one.

This case study investigates three FP7 Security Research projects – **CRISMA, SPEEDKITS and ESS** – that involved various types of partners. Drawing on the testimonies from project coordinators and participants, the case considers the challenges that have been faced in managing partners from diverse professional and disciplinary backgrounds and identifies (successful) approaches to addressing the challenges and issues faced.

F.13.2 Example projects

CRISMA is a large-scale integrating project which was set up to develop a simulation-based decision support system (Integrated Crisis Management System – ICMS) for modelling crisis management, improved action and preparedness[208]. The aim of the CRISMA System is to facilitate simulation and modelling of realistic crisis scenarios, possible response actions, and the impacts of crisis depending on both the external factors driving the crisis and the various actions of the crisis management team[209].

CRISMA (March 2012 – August 2015) has 17 participants from 10 countries and incorporates a range of beneficiary types including Research Institutes, Universities and a Training College, Private Sector companies, the Public Safety Communication Europe Forum, The Red Cross in Israel and Germany, the Finnish Met Office and an Industry Association. The project budget is €14.4m with an EU contribution of €10.1m.

The aim of the **SPEEDKITS** project[210] is to develop emergency kits to help overcome large-scale disasters. The project has produced several products to help alleviate the distress of people caught up in desperate emergencies. The products developed include new types of shelter for emergencies, a small solar lamp and the recycling of concrete from buildings demolished in disasters such as earthquakes.

Through the consortium members, the project has important input from humanitarian organisations including the Dutch Red Cross, the Red Cross/Crescent Shelter Research Unit based in Luxembourg, Médecins sans frontiers and the Norwegian Refugee Council. In total there are 16 project participants also including companies and universities. The coordinator is Centexbel, which is the scientific and technical centre for the Belgian Textile industry. Total project funding is €9m of which the EU provides €6.1m, and the project runs until the end of February 2016, having commenced March 2012.

The Emergency Support System (**ESS**) project finished in May 2013 and ran for a period of 4 years. The aim of the project was to develop a suite of real-time data-centric technologies focussed on providing actionable information to crisis managers during atypical event scenarios. The aim was to enable improved control and management, resulting in real-time synchronisation between forces on the ground..

This project involved a very large consortium, with 21 participants from 10 countries and a range of sectors, including academia, research, industry, civil society.

[208] http://cordis.europa.eu/project/rcn/102347_en.html
[209] http://cordis.europa.eu/project/rcn/102347_en.html
[210] http://cordis.europa.eu/project/rcn/103078_en.html

F.13.3 Challenges arising

The **main actors** identified in Security Research Actions can be categorised into the four main groups (see the table below). There are two supply side actors, industry and academia, and two demand side actors, the public sector and private sector[211]. In practice however, research and product development involves co-production, and both sides contribute to the concept of what is needed, and what is then provided to meet that need.

Table 67: The main actors in FP7 Security Research

Supply side		Demand Side	
Industry	Creators of the products	Public Sector	Role of customer
Academic institutions	Research provider	Private Sector	Role of end-user

Source: Manchester Institute of Innovation Research

The **different interests and priorities** of the different types of beneficiaries encompass different world views, which have to be resolved in any consortia. As the literature in the area of collaborative research identifies, increasing diversity and scale has an optimum point of efficiency for the creativity of the consortium, before the costs of coordination exceed the benefits produced.

The research action itself can be viewed as a **linear process**, from the initial vision and aims of the research, through to the outcomes and impact. Throughout this process, the diversity of a consortium can manifest itself as a challenge, but also sometimes as a benefit. Drawing on the case study interviews, the following table highlights some of the main issues faced by mixed consortia at each stage in the research process. Each is then discussed in more detail in the sub-sections that follow.

Table 68: Divergence issues across the project process

Stage	Divergence issue identified
Project vision	• Coherence and agreement of the project vision
Project inputs	• Commitment of all partners towards an agreed set of identified aims • The associated devotion of resources and skills
Research activities and outputs	• A sufficient range of capabilities required to realise the vision and aims • Agreement on ownership and knowledge sharing
Project outcomes and impact	• Continued interest and up-take • Interaction with other types of beneficiary

Source: Manchester Institute of Innovation Research

<u>Project vision</u>

The first key stage to ensure a successful research action relates to the project vision, and particularly to achieving a **shared vision** across the consortium. By default the vision is often interpreted differently by the various actors, and a central challenge for the project is to secure the commitment of all partners around a single vision, and to carry this through over the course of several years.

An illustration of the challenge can be taken from the **SPEEDKITS** project, which sought to examine and improve emergency response units including tents and shelters for crisis situations. Here, the objective from the humanitarian side was to manufacture high quality shelters at the lowest cost possible, while industry partners had a different interest and priority, which was to sell shelters for as much as the market would bear and be of a quality that would be determined by the cost. This mismatch in priorities and views between different partner types presented a challenge for the consortium, and one that had to be acknowledged, discussed and resolved at the outset to ensure a successful outcome.

[211] The private sector comprises private security services providers, as well as some types of civil society organisations such as national or international humanitarian aid or disaster relief organisations. A detailed discussion of the structure and diversity of what is called here "private sector" is beyond the purview of this case.

A further and generic challenge for all projects is that different sectors have different **motivations**. Some beneficiaries, for example, are involved through a motivation to provide benefits free of charge to their end-users or target group, while others might be focused on a consideration of profits. It is important to understand that in co-financed projects each partner has their own goals, which have to somehow be aligned with each other and with the overall and joint project goals if a project is to be successful.

Project inputs

To realise the vision of a research action requires the **commitment** of all partners towards an agreed set of identified aims, and the associated devotion of resources and skills and personnel necessary to fulfil these objectives.

The **ESS** project involved a very large consortium of 21 partners, of two main types - those delivering a service (demand side) and technology companies developing solutions (supply side). The central challenge identified by the project was to secure the commitment of the partners around a single vision and carry this through over the course of a four-year period. Reportedly, not all technology companies involved were equally committed. It was reported that in consequence there were teams lacking senior staff..

Research activities and outputs

An acknowledged problem of dealing with diversity in team-based research projects is the issue of '**language'.**[212] Where consortia comprise researchers, practitioners and industry the challenge is to develop a common understanding between team members who are not only from different countries, but also from different sectors, and who normally, do not speak the same language or use the same terminology

Finding shared **tools** to facilitate communication is also not straight forward amongst teams from different sectors. For example, and as pointed out by CRISMA, common freely available software such as Skype and Dropbox used much in academia are often not acceptable to industry, due to security concerns.

One output challenge more specific to Security Research Actions is the **sensitive nature of some of the research** being undertaken, and the different stances partners take with regard to openness and ownership of IPR. For example the incentives for academic partners are to share data, information and knowledge and to publish their findings widely, whereas industry partners, particularly in the security related sectors, are more conservative. This can limit publication opportunities for beneficiaries. Also, project deliverables or results may be classified (i.e. represent EU Classified Information, where specific rules and conditions apply).

Project outcomes and impact

One main challenge identified by the **CRISMA** project is what happens at the end of the project. Some partners may **lose interest** in commercialisation and without a clear strategy (i.e. a capability and commitment), there may be no exploitation of findings. The project (and all its partners) may see few if any of the expected outcomes as a result, and therefore little or no impact.

Another aspect concerns the **opportunity to work with a wider range of partners** (in other European countries) in addition to those project partner traditional collaborate with. As was the case for SPEEDKITS for example, the opportunity and benefits of direct engagement with private sector actors were appreciated by the humanitarian side. The inclusion of more industry partners was even recommended, as – although translation across sectors is not easy – the benefits are worthwhile and the impact significantly enhanced.

[212] Ettorre, E. (2000) Recognizing diversity and group processes in international, collaborative research work: A case study. *Social Policy & Administration,* 34(4), 392-407.

F.13.4 Good practice solutions

Emerging from the study of the Security Research projects above are a number of good practice solutions that have been suggested by project interviewees.

Before, and at the start of projects, it is important that members of the consortia have an **organisational commitment** to the outcomes of the project, and that they appoint the following kinds of people to be involved: relatively senior staff; technically competent people; people who are willing to work with others (team players). The full commitment of all partners is essential, even if the project changes shape or priorities as it proceeds through the various delivery stages.

In addition, **building a common vision, culture and language** within the project team is considered to be important by those interviewed for this case study. An essential step is to hold intensive meetings with the entire consortium at the outset of the project. For example, in one case there were three such meetings, lasting 3-5 days each in the first three months of the project. While this implied a significant time commitment for the partners, it was seen as beneficial for the delivery of the project, and considered to actually save time in the long-run.

Firm leadership is another success factor for the management of diverse project teams. This means a coordinator who has strong management and coordination skills and experience, as well as a 'vision for success', who can secure the commitment of other partner organisations. Such a project manager also needs to be flexible enough to cope with the inevitable need for the project to evolve during the course of its lifetime. However, at the same time, it is important for partners not to be over-managed. For example, the introduction of a 3-monthly reporting cycle, as practiced by some projects, might be counterproductive.

The projects examined also found that outcomes and impact can be facilitated if a **strategy for commercialisation** and marketing is pre-prepared at an early stage (even prior to the project commencing). Evidence of this planning could also be cited in the application for funding to show a serious intent towards commercialisation of project outputs. It is here, where the composition of the project team is crucial. To incorporate partners that can realise the vision and deliver the products envisaged has been instrumental for the success of some projects. At the very least the consortium should have in place a plan to deliver the outputs should the consortium partners not be able to do this directly.

F.13.5 Conclusions and lessons learnt

The scale and shape of the project consortium for successful collaborative activity has been the subject of much previous research. Drawing on a sample of interviews with Security Research Action participants, this case study has elaborated some of the challenges of managing diverse project settings involving different types of partner and has identified some examples of good practice.

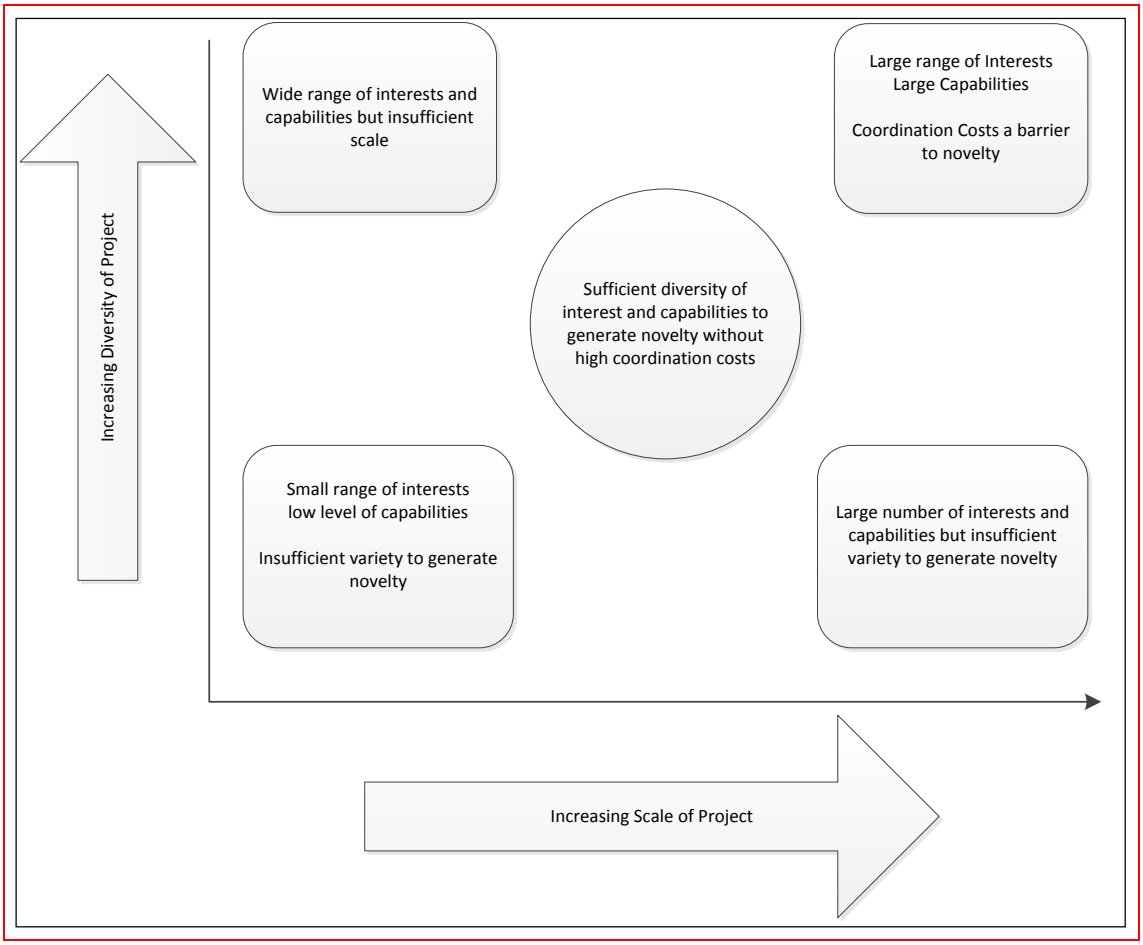
The **challenges** that have been identified include: achieving a shared vision; aligning/ accommodating differing expectations, priorities and world views; securing the right skills and capabilities, and making best use of these; achieving a common language and means of communication; and (for some actions) dealing with commercialisation and confidentiality issues before they arise.

From the examination of example projects, the case identified three **key factors** for managing successful diverse Security Research Actions. These relate to ensuring a **shared commitment**, a **common understanding** and a **common language**. Essentially how well project partners work together will depend upon individual personalities and the relationships between those individuals. The onus in a successful consortium is, to a large extent, on the coordinator/manager to facilitate good team bonding, combined with effective communication and to ensure the maintenance of good working relationships.

More broadly and on a theoretical level the case study suggests a concept that there may be an **optimum level of scale and diversity** in projects, beyond which both efficiency and benefits decline. Figure 35 below attempts to illustrate this. It is a simplification, but should convey some of the important lessons of the case about the challenges that may arise related to project team size.

- Close to the lower left corner of the figure there are small scale, low diversity projects. Here control is easy but the generation of creativity and novelty is low. Moving out along both axes there are either high diversity projects at low scale or low diversity projects at large scale. In neither of these cases are projects capable of generating sufficient novelty while at the same time being manageable.
- Larger projects in terms of diversity and size may have significant capabilities and a wide range of interests, but are difficult to coordinate and the costs of managing them in terms of time and effort may simply be too high. Indeed, the sheer scale of such projects may be so big and the diversity so large that agreement within the project (e.g. on priorities) is not possible. This is suggested by the SPEEDKITS project for example where for-profit and non-profit motivations were highlighted.

Figure 35: Project optimisation – an idealisation



Source: Manchester Institute of Innovation Research

Several lessons have emerged that can be used to address the specific challenges of diverse project settings involving numerous types of partner, and might also be generalised for H2020.

It is imperative that a consortium **resolves the different world views** of its members to align with the project outputs and to agree the dissemination of those outputs. This should be achieved in the early stages of the project. One central goal is to avoid that partners collide – e.g. those driven by considerations for profit and those motivated by non-profit aspect – on not only the dissemination of products produced but also on the processes to generate those products.

Closely related to this is the need for project beneficiaries to **align their vision** of the project from the outset and in so doing eliminate some of the inherent tensions that exist in large, multi-partner consortia. An initial exploration of how partners perceive project aims and their own role can take place at the first meeting.

Investment in **professional, experienced management** of large, diverse research project teams is essential for success and to overcome the challenges inherent in the complexity and nature of such work. A dedicated management resource facilitates the successful running of these research teams and their associated stakeholders and communities, and is an essential pre-requisite for a positive project outcome. This person or management team needs both technical understanding of the project and understanding of the cultural differences in the partner countries and in the partner sectors.

An initial commitment from the full project team to dedicate to **total immersion in consortium meetings** at the outset of the project over a period of several days has proven successful. It establishes the baseline of activity without at this stage bringing in too much new material and brings together the team to effect communication and closer collaboration. Professional and committed project management is a pre-requisite for the bringing together of the consortium to these intensive meetings. Such early lengthy and immersive meetings demonstrate to partners the **required commitment and active participation**. The larger and more diverse the project consortium the more face-to-face meetings will be needed in the first 6 months of the project.

F.14 The significance of standardisation for Security Research Actions

The objective of **this case study** is to assess whether standard is an important part of FP7 Security Research projects and how the programme has managed to contribute to reducing the fragmentation of the security market through the development of standards. The case study puts more emphasis on projects that have involved **standardisation organisations** – as they seem to be key players in pushing for standards. It contributes to the evaluation of the programme's effectiveness in improving coherence and overcoming fragmentation.

The case first introduces the problem of market fragmentation in the security sector and the potential of the use of standards to help address it. It then examines projects with a "standards dimension" before focussing on the subset of projects with a standardisation organisation as partner. The conclusion summarises the outcome and impact of the standards projects and looks at lessons from the involvement of standardisation organisations, as well as lessons for Horizon 2020.

This case study is based on desk research, analysis of CORDA data and five interviews with representatives from four standardisation organisations and the European Commission.

F.14.1 Introduction

An essential feature of security market is that it is a highly fragmented market, lacking harmonised certification procedures and standards. The main reason for this is that large parts of products and services end-users are national authorities (civil security, law enforcement forces, boarder control forces, etc.). National interests are much stronger than in other industrial fields. This aspect reinforces the fragmentation of a market that is already small, given the limited target groups potentially interested in these products and services (niche markets rather than mass markets). Yet overcoming market fragmentation is essential to increase the global competitiveness of the EU security industry. To address these difficulties the European Commission launched a dedicated initiative on an **EU Security Industry Policy** including an **Action Plan for an innovative and competitive security industry**[213]. Through this initiative, the aim of the Commission is to foster the European internal market for security technologies.

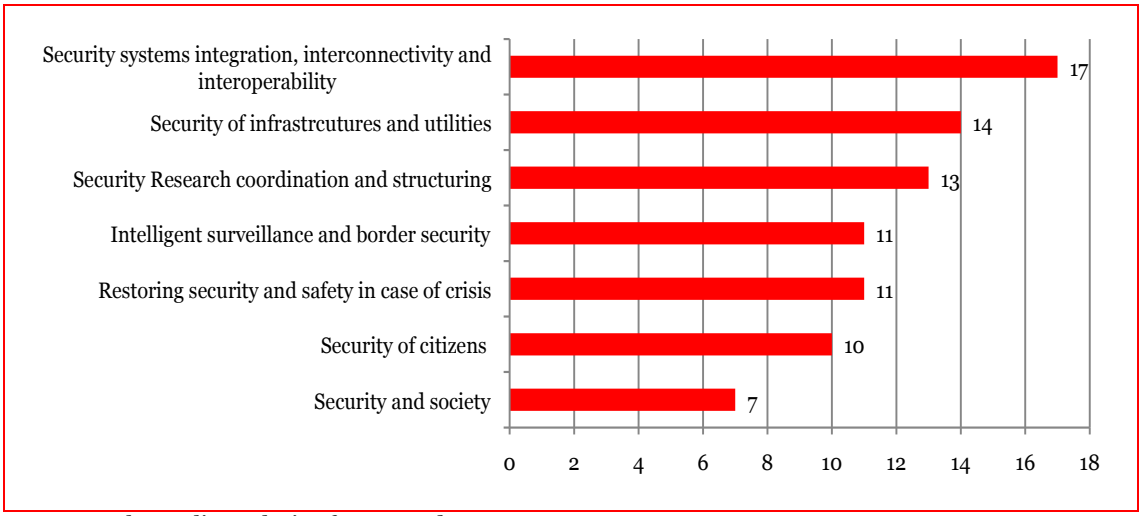
The FP7 Security Research Actions cover very different topics in the field of security, with some focusing on technology development and other rather focusing on interoperability or "social" aspects of security issues. In these various fields, **standards can help to reduce market fragmentation** and **improve interoperability** between national systems (border control, database, communication, crisis management protocols, etc.). Standardisation bodies are promoting **standards as a complementary tool for dissemination**: by setting standards on emerging issues, consortiums can pave the way for concrete dissemination of projects' outputs and can push for a higher use of IP made from projects outputs.

F.14.2 Projects with a "standards dimension"

In the FP7 Security Research project portfolio, 83 projects have a direct or indirect link with standards (i.e. the word "standard" is mentioned in the projects' abstract). When considering the distribution of projects with a "standard" dimension (see the figure below), the three most represented missions are "Security systems integration, interconnectivity and interoperability" (17 projects, i.e. 20%), "Security of infrastructures and utilities" (14 projects, i.e. 17%) and "Security Research coordination and structuring" (13 projects, i.e. 16%), whereas only "Security of infrastructures and utilities" (with 17 % of projects) is part of the three most represented missions at programme's level. "Security systems integration, interconnectivity and interoperability" and "Security Research coordination and structuring" represent only around 10% each of all the projects funded under the Security Research Actions scheme.

[213] COM(2012) 417.

Figure 36: Distribution of projects with a "standard" dimension by mission



Source: Technopolis analysis of CORDA data, January 2015

In these 83 projects, the "standard" dimension can take the following forms:

- **Research based on current existing standards** ("document a review of current CP methodologies and BCM from various sources, encompassing international, national and domain-specific standards and guidelines[214]");
- **Standards mentioned as a possible output of the research project** ("recommend a relevant strategic research roadmap including standards[215]");
- **Evaluation of the need for standards** ("there will be a need to set agreed upon tasks, operational procedures, standards, user requirements for the PPE[216]");
- **Standard used as an equivalent for "values"** ("to identify human rights and other legal and moral standards that detection technologies in counter- terrorism must meet[217]").

However, the 'standard' dimension is mostly a minor subject in these research projects, which leads to very limited outputs on standard in most of these 83 projects. This shows two things:

- There seems to be a discrepancy between the push from public bodies (Mandate 487 issued by the European Commission to ask European Standardisation Organisations (ESOs) to develop roadmaps and standardisation strategies in the field of security) to work and standardisation and the actual involvement of industrial stakeholders in standardisation activities in research projects;
- The "standard" dimension in proposals is often limited and is not considered a priority for most of the consortia working on FP7 Security Research projects. Standardisation bodies consider that the number of projects with actual standardisation content is very limited.

[214] EURACOM: http://cordis.europa.eu/project/rcn/92076_en.html

[215] OPERAMAR: http://cordis.europa.eu/project/rcn/86254_en.html

[216] NMFRDISASTER: http://cordis.europa.eu/project/rcn/88082_en.html

[217] DETECTER: http://cordis.europa.eu/project/rcn/89373_en.html

F.14.3 Projects with a standardisation organisation as partner

Among these 83 projects, 9 have benefitted from the participation of one or two standardisation organisations. The distribution of projects with a standardisation body by mission is as follows:

Table 69: Distribution of projects by mission

Missions	Projects	Bodies
Security Research coordination and structuring	CRESCENDO	AFNOR
	ESCORT	CEN, UNIFENDO
Restoring security and safety in case of crisis	INDIGO	CEN
	PRACTICE	CEN
	DRIVER	DIN
Increasing the Security of the Citizens	TIRAMISU	CEN
	D-BOX	CEN
Security of infrastructures and utilities	SAFEPOST	NEN
Security systems integration, interconnectivity and interoperability	CRISP	NEN

Source: Technopolis analysis of CORDA data, January 2015

These projects focus on different areas, and this has implications in terms of standardisation work:

- Some projects focus on **potential and needs for standards** (or certification), with a focus on building a standardisation strategy rather than standards (CRESCENDO and CRISP).
- Some projects focus on **technology** (ESCORTS and SAFEPOST).
- The majority of projects focus on **process**, in the field of demining (D-BOX and TIRAMISU), crisis management (INDIGO and DRIVER) and CBRN (PRACTICE).

For projects focusing on technology or process, the objective regarding standardisation is to consider standard as a potential dissemination activity and to work towards the establishment of a standard.

Standardisation bodies intervene in projects with a specific role:

- In prospective projects (i.e. projects that aim to identify needs in the field of research): the reason for standardisation bodies to participate is to provide inputs on what can be a standardisation strategy in one specific area. It was the case for the CRESCENDO project[218], focusing on the way to reduce the fragmentation of the European security market.
- To provide expertise on the standard dimension of a project: the various issues related to standardisation are not always well known among project partners. The standardisation body's role is to provide the consortium with a framework for intervention:
  - On general consideration: What is a standard? What are the procedures to follow in order to produce a standard?
  - On specific aspects: the standardisation body provides the consortium with support towards standardisation work that can lead to a CEN[219] Workshop Agreement for instance. For example, in the INDIGO project[220], the role of CEN was to "provide the consortium with both the expertise and support in the field of standardisation for the emergency symbology[221]".

[218] http://cordis.europa.eu/project/rcn/91164_de.html

[219] CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 33 European countries. CEN is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association.

[220] http://cordis.europa.eu/project/rcn/107681_en.html

[221] http://indigo.diginext.fr/EN/index.html

Only four out of these 9 projects were completed by December 2014. These projects have led to different outputs in terms of standardisation: guidelines on a standardisation strategy, with the identification of priority areas and demand (or lack of) for specific standards, CEN Workshop Agreements, pre-standard works, etc. For the projects that were focusing on interests and needs for standards, the results are in line with the expected outcomes. For the other projects, **standardisation work has to be followed up** by work among partners as well as with standardisation organisations, in order to turn projects outputs into international standards.

The participation of standardisation organisations (and the dedication of other partners to work on the issue of standardisation) is an efficient way to raise awareness among all partners on the issue of standardisation, build a coherent standardisation strategy and to ensure the follow up of this activity, even after the end of the project. However, whether it is CEN/CENELEC[222] or a National standardisation organisation involved in the project, **a standardisation organisation cannot build a standardisation strategy by itself**: the process for standardisation is a participatory process, meaning stakeholders from different background (policy makers, industrial, academia, consumers, etc.) have to participate in the definition of a standard. This has a consequence: **participants other than standardisation organisation have to plan to dedicate resources to this activity** when drafting the proposal.

F.14.4 Conclusions and lessons learnt

This case study allows to draw conclusions with regard to the outcomes and impacts of FP7 Security Research projects on standards, with regard to the involvement of standardisation organisations and to formulate lessons learnt for Horizon 2020.

Even though a large number of projects referring to standards in the project's abstract are not finished yet, it is possible to draw some conclusions on the significance of standardisation for security research actions:

- A relatively high number of projects have made references to "standard" in the abstract, but for the majority of these projects, the actual planned **work on standard is limited**, especially because there is no resource dedicated to the issue. A lot of participants have a limited knowledge of the usefulness of standards (for instance as a way to build a coherent IPR strategy) and on the processes to follow to achieve standard activities;
- Security Research Actions have however led to some interesting work in the area of standardisation, especially because projects have contributed to **identify gaps and needs for standards**, thus contributing to working towards reducing market fragmentation of the EU security market and to improve interoperability (for instance through the development of international common symbols for First Responders);
- The **participation of standardisation organisations** (and the dedication of other partners to work on the issue of standardisation) is an efficient way to raise awareness among partners on the issue of standardisation, build a coherent standardisation strategy and to ensure the follow up of this activity, even after the end of the project;
- Among the 9 projects that involved a standardisation organisation, one – CRESCENDO – had a **direct impact on EU priorities regarding standardisation** in the field of security. CRESCENDO provided guidelines for the European Commission, by identifying needs. This was used as an input for **M487**, which led ESOs to focus their work on the following topics: Chemical, biological, radiological, nuclear and explosives (CBRNE), border security, crisis management/civil protection. Overall, projects seem to be in line with EU priorities, especially in the field of crisis management. The concept of hybrid standard (applicable to civil security and defence) has however not been developed so much, even

[222] CENELEC is the European Committee for Electrotechnical Standardization and is responsible for standardization in the electrotechnical engineering field.

though the European Commission has planned to issue standardisation mandate to ESOs on the subject[223];

- At international level, a new committee was launched on 1st January 2015 by the International Organization for Standardization (ISO): ISO/Technical Committee 292 Security and resilience[224]. The launch of this committee is the result of the **increasing demand for standards on security at international level**. Among the 27 members of the committee, all the biggest EU countries are represented. The focus of this committee has common features with the FP7 security research programme (societal security, supply chain security, risk management, etc.). The objective is to develop a general model for broad security standards, with sector-specific issues dealt with in more specific technical committees. The creation of this new committee is an opportunity for EU stakeholders to make their work used to set up international standards. This could be done by increasing the link between project partners and standardisation organisations.

According to standardisation bodies (at European or national level), the only way to produce standards or standard-related outputs from a FP7 Security Research project is to **dedicate time and budget to this issue**, and not only time for a standardisation body: Standardisation bodies can only have an advisory role; stakeholders (within or outside of the project) have to dedicate time to build a common agreement.

National standardisation bodies have been active in **communicating towards the Security research community** (both academia and industrial partners) on the potential for standardisation as part of the dissemination process of their projects. As a result, these national bodies have received more questions on ways of including standard work on their research projects.

By participating in projects, standardisation organisations can undertake the **liaison** between stakeholders involved in research projects and technical committees, at national, European or international levels.

There are a number of **lessons that can be drawn for H2020**.

- First, dedicating resources to standard-related work in a project is a good way to ensure real standard-related outputs emerge from the project. Resources should be i) time for all consortium members to participate in activities related to standardisation and ii) budget for the participation of a standardisation body in order to give guidance on the process.
- This means that already during proposal evaluation, evaluators should review how the consortium has planned to dedicate time for working on standard-related issues and on what level, standardisation bodies will be involved in the process. Without these two elements, the experience shows, standard-related activities are likely to be (very) limited.
- In order to improve the impact of FP7 projects on standards, European and national standardisation organisations should keep communicating towards participants on the process and potential outcomes of standardisation. Raising awareness among partners is an efficient way to push for more standard-related activities in future projects.

[223] CHENARD, B. (2014) EU Security Industrial Policy & Standardisation – Strengthening Science- Policy-Industry links in the CBRN-E sector (presentation).

[224] ISO (2015), ISO/TC 292 Security and resilience.

F.15 The influence of FP7 SRAs on national research programmes

This case study examines the relationship between the FP7 Security Research Actions (SRA) and national security research programmes in order to contribute to the analysis of the European added value (EAV) of the FP7 Security Research.

This case study is **structured** as follows: The first section provides a brief introduction to the concept of EAV, followed by an overview of national security research activities, be it in the form of a dedicated security research programme or alternative forms. The subsequent sections are dedicated to a description of three national security research programmes in particular (in Austria, France and Germany), and their relationship to the FP7 Security Research programme. Finally, the case study presents conclusions as well as the EU added value and lessons for Horizon 2020.

The case study is based on a desk research, interviews with seven experts from four different Member States and resulting analysis.

F.15.1 Introduction

EAV concerns benefits that cannot reasonably be achieved by the actions of individual Member States (MS) or private actors, or which are likely to be substantially greater if pursued at EU level, rather than nationally or through some narrower territorial alliance. It points to the broader European relevance and significance of a programme for the EU, its institutions and policies. EAV is therefore paramount in the formulation of the objectives and underlying ideas of EU RTD Framework Programmes.

Part of the consideration of the existence, or not, of EAV concerns the coherence of research actions undertaken at MS and EU level, and in particular the extent to which these actions are complementary, overlapping or duplicative.

Using the examples of national security research programmes in Austria, France and Germany, the **case study analyses** the following aspects:

- The structure of these national programmes, the areas they address and whether they deal with the short- or long-term needs of users
- The link between the FP7 SRA and these national programmes
- Overlaps or complementarities between the FP7 SRA and national programmes
- The added value of the FP7 SRA, compared with MS security research activities

F.15.2 Security research in Member States

There are a number of EU countries with considerable **security research activities**. In some cases this research is carried out through dedicated national security research programmes, but more often it forms part of wider security or research strategies. A brief overview of the different approaches taken by a number of Member States is presented below.

- In **Poland**, the National Research Programme[225] highlights 'state security' as one of seven important strategic areas, while the National Security Strategy[226] specifically addresses research within the security area.
- In **Sweden**, there is a comprehensive research programme for a safer society, which incorporates security-related issues[227]. Sweden also launched a specific programme on security research in 2010, but this was discontinued in 2013[228].

[225] National Research Programme – Assumptions for the Science & Technology and Innovation Policy of the State.

[226] National Security Strategy of the Republic of Poland.

[227] See Forskning för ett säkrare samhälle: ny kunskap för framtidens utmaningar MSB:s forskningsstrategi 2014–2018.

[228] Knowledge to Safeguard Security, Vinnova. VP 2005:03, 2005.

- In the **Netherlands**, there is an innovation programme 'Secure by Innovation'[229], which includes funding for research on end-user needs. This includes a focus on specific end-users (such as fire fighters) that are related to the security field.
- In the **United Kingdom**, there are research activities related to security that are supported by different government departments[230]. Additionally, there is a National Security Strategy[231] and a Science and Technology Strategy for Countering International Terrorism[232], which aims to use innovation, science and technology to reduce the risk to the UK and its interests overseas from international terrorism.
- In **Italy,** the National Research Council (CNR) oversees an interdepartmental security project, and maintains a technological platform for national security research with the company Finmeccanica[233].

In the mid-2000's, several EU Member States established a dedicated **national security research programme**. The creation of national security research programmes was called for by the Commission. Currently there are four EU Member States with specific national security research programmes, as follows:

- Austria: Österreichische Förderungsprogramm für Sicherheitsforschung *KIRAS* (National Research Development Programme)[234]
- France: Concepts, Systèmes et Outils pour la Sécurité Globale *CSOSG* (Concepts, Systems and Tools for Global Security)[235]
- Germany: Sicherheitsforschung – Forschung für die zivile Sicherheit (Security Research – Research for Civil Security)[236]
- Finland: The National Security Research Strategy[237]

Three of these national research programmes are presented in more detail in the next section. The research programmes of **Austria, France and Germany** have been selected because of their significance and the fact that they are dedicated national programmes that have been set up to align with the goals and ambitions of the FP7 Security Research Actions. Representatives from the three countries concerned have also been very active in cooperating with the Commission through their work in the Programme Committee, in particular as members of the so-called 'Group of Six' (see further below).

F.15.3 Three national security research programmes

The Austrian, French and German national security research programmes are introduced in turn below. In each case, this includes information on the design and implementation of the programme, as well as its objectives, general orientation, budget and the number of projects funded. Specific characteristics of each programme are highlighted, while the influence of the FP7 SRA, and the complementarity between the European programme and individual national programmes are also explored.

---

[229] Innovation Agenda for Security and Justice, Ministry of Security and Justice.

[230] See for example the activities of the Academic Centres of Excellence in Cyber Security Research (ACEs-CSR).

[231] HM Government (2010) A Strong Britain in an Age of Uncertainty: The National Security Strategy, London.

[232] HM Government (2009) The United Kingdom's Science and Technology Strategy for Countering International Terrorism, London.

[233] Platform for National Security Research.

[234] http://www.bmvit.gv.at/en/innovation/security_research.html.

[235] http://www.agence-nationale-recherche.fr/suivi-bilan/ingenierie-procedes-securite/concepts-systemes-et-outils-pour-la-securite-globale/.

[236] http://www.bmbf.de/en/6293.php.

[237] http://www.intermin.fi/download/14209_national_security_research_strategy_.pdf?31652d691c05d188.

The Austrian security research programme

The Austrian security research programme (Österreichisches Förderungs-programm für Sicherheitsforschung – KIRAS) was the first national security research programme in Europe. Being strictly separated from defence research, the programme is managed by the Federal Ministry for Transport, Innovation and Technology.

KIRAS supports national research projects whose results contribute to the security of all members of society[238]. It has five strategic **objectives**:

- To enhance the security and awareness of citizens about safety and security
- To generate knowledge that is required for security policy
- To achieve development leaps regarding security-related knowledge, processes and technologies
- To contribute to the growth of the domestic security industry
- The establishment and development of excellence in the field of security research

Finally, the projects funded under KIRAS are also intended to contribute to the creation of skilled jobs in Austria.

KIRAS builds on an **integrated approach**, in the sense that it does not only fund research on technological solutions, but also promotes security research from the perspective of the social sciences, cultural studies and humanities. In two of its programme lines ('explorative projects' and 'collaborative projects') it requires the active involvement of end-user, research and industrial organisations, as well as of researchers from the social sciences and humanities.

During **2006-2013** there were 21 different calls within the programme and the number of funded projects during the period was 172. The total funding for this period was approximately **€58 million**. According to interviewees, the projects funded through the national programme are comparable to FP7 projects, although they are slightly shorter in timescale.

The programme has a strong focus on funding national research, and it puts emphasis on ensuring that results can be utilised in industry and public administration. The programme also emphasises an active involvement of **end-users**, in particular of procurement organisations, and to this end it is a requirement that at least one end-user participates in each project.

According to those interviewed, the experience gained from KIRAS-funded projects has shown that end-users need to be deeply involved in the projects in order to make the results useful and applicable in society. However, the involvement of end-users has not been without **challenge**. In particular, end-users highlight that they find it difficult to allocate resources and time to the projects, and sometimes lack long-term planning for the procurement of new technologies. These findings are in line with the results of the stakeholder interviews and surveys conducted for the purpose of the evaluation outside of this case study.

The Ministry for Transport, Innovation and Technology has made a major effort to **adapt the National Programme to the FP7 Security Research Actions** in order to better prepare Austrian actors for the participation in both. As a result, topics addressed in KIRAS include some that have also been addressed in the FP7 Security Research programme.

There are also examples of specific projects that, having started with funding through the national programme, were then scaled up and became a European project funded under FP7. One example of such a project is the national project on airport screening techniques, FBC – *Grenzkontrolle der Zukunft*[239], which was developed further under FP7 in form of the project FastPass[240].

[238] BMVIT (2015) Sicherheitsforschung.

[239] KIRAS (2010) FBC – Future Border Control.

[240] http://cordis.europa.eu/project/rcn/106743_en.html

The French Security Research Programme

The French Security Research Programme (Concepts, Systèmes et Outils pour la Sécurité Globale) was **launched in 2006** and is managed by the French National Research Agency (ANR), in cooperation with the Direction Générale de l'Armement (DGA) and the General Secretariat for Defence and National Security (SGDSN).

The **objectives** of the national programme are:

- The protection of the citizen, which includes in particular the fight against terrorism and crime
- The protection of critical infrastructure and services (especially in urban areas), and networks (transport, energy, IT…) and their interconnections
- Crisis management, regardless of its origin (malice, natural or accidental), and the resilience in the preparation, planning, relief and recovery phases
- The fight against cybercrime

The Programme aims to develop applicable solutions, taking into account ethical considerations, the acceptability of systems and respect for privacy. The research must in particular contribute to the development of industrial sector security solutions and to the creation of jobs in France.

Since 2006, the programme has provided approximately **€120 million** in funding to around 100 projects[241]. The **time horizon** of the programme's activities has varied: Interviewees point out that sometimes short-term needs were addressed, and sometimes longer-term needs. Examples of addressing short-term needs are, for instance, related to technology breakthroughs, or when there has been a need for smaller projects in order to be able to involve end-users. The ambition for the latter was to launch a smaller project as a first step and in a second step to up-scale the project to become more extensive at a European level.

One ambition of the French programme has been to find a good **mix** of topics. In particular, it has been important to put an emphasis on the needs of end-users and to answer to the needs of industry and the academy. In order to identify these needs, the Research Agency worked with clusters of individuals (e.g. from industry), which those consulted for this case believed was a process that worked well.

According to interviewees, since the launch of the national security research programme, an effort has been made to **synchronise** it with the FP7 Security Research programme. Because participants were not always experienced in the area of security research, the French strategy was to initially launch projects at the national level. However, there are now projects (for example one on maritime surveillance), which started under the French programme and later continued as a FP7 Security Research project.

The national programme was also **reformed in 2013**[242], when research programmes funded by the National Research Agency were reorganised according to the different challenges in Horizon 2020. This approach is also outlined in the new research strategy: *Stratégie nationale de recherche – France Europe 2020*.[243]

The German Security Research Programme

The German security research programme (Research for civil security 2012-2017) is managed by the Federal Ministry of Education and Research. It seeks to develop innovative solutions that increase civil security, while balancing security and freedom.

[241] L'Agence nationale de la recherche Annual reports 2006-13: http://www.agence-nationale-recherche.fr/en/information/documents/annual-reports/.

[242] L'Agence nationale de la recherche Annual report 2013: http://www.agence-nationale-recherche.fr/fileadmin/documents/2014/ANR-Annual-Report-2013-150dpi.pdf.

[243] Ministère de l'Éducation Nationale, de lÉnseignement Supérieur et de la Recherche (2013) Stratégie nationale de recherche - France Europe 2020.

The programme is structured according to **three missions**. The first is scenario-oriented research (that stresses the needs of end-users), while the second focuses on cross-sectional research, and the third focuses on international cooperation.

The funding **priorities** for the programme are:

- Societal aspects of civil security
- Urban security
- Infrastructure and business security
- Protection and rescue of people
- Protection from hazardous substances, epidemics and pandemics

One of the main **achievements** of the programme has been the establishment of networks of end-users, as well as joint networks of end-users, companies and research organisations. Furthermore, focus has been put on specific end-users such as fire fighters, as well as areas such as infrastructure protection. These kinds of links and networks did not exist prior to the establishment of the national programme.

The programme has also insisted on **systematically involving social science** in security research. Social science contributions cover a wide range of topics from privacy issues and data protection, perceptions of security and economic aspects, to the institutional settings of security. The latter, in particular, can be of crucial importance for the provision of new security services or the application of new technologies. Sometimes they hinder cross-border collaboration or the creation of a pan-European market for security products and services, e.g. when different legal requirements or technical specifications apply for the same type of equipment or for their use. Hence, increased attention is paid to understand and shape these 'framework conditions' of security.

Since 2007 the Federal Government has spent **€400 million** and funded around 160 projects within the national programme[244]. This represents significantly more money per project than in the other EU countries examined for this case study. The duration of research projects is comparable to FP7 SRAs.

Those interviewed for this case study consider the national security research programme to be **complementary to FP7 Security** Research in three ways:

- Projects funded under the national security research programme are considered to be the first step for research in an area, which may be later complemented by projects funded through FP7. This notion is similar to that held by Austrian and French experts consulted, and has to be distinguished from the practice of preparing national players to be more successful in EU proposals.
- The German national programme and the FP7 SRA are also considered to complement each other in terms of their technology readiness levels (TRL) focus. Internal market legislation generally allows national governments to fund research and technology projects up to the demonstration stage. The Commission can continue funding research and technology projects at higher TRL levels, closer to the market stage, and has instruments for further follow-up, e.g. as regards standardisation and certification efforts. The solution developed with national funding may then gain access to the larger European security market, especially in cases where FP7 funded projects are working towards or preparing European standardisation and certification activities. In other words, while both programmes fund research projects at lower TRL, only the Commission has the instruments to fund innovation projects closer to the market. The national funding does not aim to fill the gap between research and the market. The risk of violating common market rules on procurement is a main reason for this orientation, according to the experts interviewed for the purpose of this case study.

[244] BMBF (2014) National funding for security research.

- Both programmes also complement each other when it comes to the establishment of networks among different types of actors - research organisations and companies - in the security research field, and importantly also between these two types of actors and end-users. While the national programme has been instrumental in establishing these kind of networks in Germany, the FP7 Security Research Actions have promoted cross-border and pan-European networks.

As regards the **time horizon** of the funded projects, the German national programme and the FP7 SRA are aligned, as they both address mid- to long-term needs and address similar research topics. Short-term 'research' or rather 'innovation' needs are addressed in Germany through the functional ministries or agencies, such as the organisations responsible for interior security, border security or disaster relief.

To ensure the **valorisation** of research results, each project funded by the national research programme is required to include a work package on dissemination and exploitation, similar to projects funded under FP7. The focus is more on exploitation of the output than on the dissemination of information about the research results. Moreover, the efforts concern the last period of funding, as well as the first two years after the end of the project. In contrasts to projects funded through FP7, there is a follow-up by the Ministry, with the success of dissemination efforts evaluated two years after the end of the project. Hence, project leaders have a stronger incentive to disseminate their research results and foster their application.

F.15.4 Networking and cooperation among countries with national security research programmes

Several Member States coordinate their respective security research activities. For example, Germany and France, and Germany and Austria have formally agreed to collaborate on security research and support cross-border projects. Member States also increasingly collaborate on developing a common position vis-à-vis the Commission and to the shaping of the FP7 Security Research Actions agenda through the Programme Committee. In particular an informal 'Group of Six' Member States has played a role in this regard.

The cooperation of the informal **Group of Six** (Austria, France, Germany, the Netherlands, Sweden and the United Kingdom) started around 2006, in connection with the work on the Preparatory Action for Security Research (PASR). Initially representatives of these countries met to share experiences regarding security research. However, the group has gradually moved its focus towards developing joint research priorities for the Commission and discussing strategic issues and priorities in security, linked to security research under the EU Framework Programme. The group meets informally before the meetings of the Programme Committee and have, on several occasions, drafted common position papers.

The representatives of the countries point out that the Group of Six is **not a formal group** or network, which would be ruled by official documents or mandates. Sometimes the countries have formulated common standpoints, while at other times they have different standpoints. Usually, however, they form their opinion before the meetings of the Programme Committee and speak there with one voice.

F.15.5 Conclusions and lessons learnt

The national programmes of Austria, France and Germany focus on their national needs for security research and development. This is also in line with the different threats and risks encountered or perceived by the different nations and the priorities for their respective national security policies. They do share a holistic and all-hazards **approach** to security, even though the structure of the programmes differs.

Common to all three programmes is the **aim** to support national security research organisations and to promote the domestic industry. The latter goals are well aligned with the objectives of the FP7 Security Research Actions. An important objective of the programmes in both Austria and France has been the creation of new jobs.

Looking across the activities of the different programmes (see table below), each has funded between 100 and 200 projects over a 6-8 year period. However, the overall budgets involved, and the cost per project varies considerably.

Table 70: Number of projects and governmental contributions to security research from 2006 - 2013 (approximate values)

Country	Governmental contributions in million €	No. of projects	Average contribution per project in million €
Austria	58	172	0.3
France	120	100	1.2
Germany (2007-2013)	400	160	2.5

Source: Technopolis

Regarding **time-horizon**, anecdotal evidence suggests that the national programmes have tended to address the shorter-term needs, compared to the longer-term perspective of the FP7 Security Research Actions. In other words, the actions at EU level are in some cases being complemented by the programmes at national level. The national programmes have in particular focused on encouraging participants to fine-tune their projects in line with the needs of the end-users.

According to this analysis, the national programmes have undoubtedly contributed to **strengthening networking and cooperation**, both within the individual Member States and between them. The experiences from the national level have influenced the FP7 Security Research programme, while the European programme has influenced Member States' national security research programmes.

In conclusion, this reciprocal development of the FP7 Security Research programme and the national security research programmes has contributed to an overall strengthening of security research in the European Union.

Regarding the **European added value** of FP7 Security Research Actions, the examination of national security research programmes supports the results of the stakeholder interviews and participant survey conducted as part of the evaluation outside this specific case study.

In particular, there are several examples of added value from FP7 Security Research as compared with MS security research programmes.

- There are topics that are better addressed by security research activities in an EU context, like efforts towards standardisation and certification, since it is very costly for each country to address this on a national level. Moreover, different national approaches to these topics would imply the fragmentation of the security market.

- Generally, there is a sense among interviewees that the supply and demand sides of the security market are very fragmented across the EU. Consequently, there are few economies of scale on either side of the market. Here the FP7 Security Research programme has brought added value and complemented national security research programmes.

- Interviewees also highlighted that a particular European added value of the FP7 SRA relates to addressing cross-border issues and challenges of interoperability.

The analysis also supports the findings of the other strands of analysis with regard to **coherence, as there is little overlap** between the European and national security research programmes. Moreover, experience, competence and results from projects funded on the national level have transferred to, been used by and been built upon in FP7 Security Research projects, which also brings added value to the FP7 Security Research programme.

On the basis of the analysis of national security research programmes, several **lessons might be drawn for Horizon 2020**.

- In particular, the mandatory involvement of end-users in all security research projects funded under H2020 would have the positive effect of ensuring that these projects respond better to the needs of end-users. Moreover, systematic efforts during the last phase of research projects and in the years thereafter should be undertaken to make research results known to a larger community (including end-users). To this end the Commission should closely collaborate with the Member States.

- **Complementarity** between national and EU level security research activities could also be improved in three ways:
  - National and EU-level security research programmes should systematically complement each other, with EU efforts **focusing on the last TRL before market entry**. While both, European and national security research will always fund research on lower TRL, the Commission is particularly well suited to support research on subsequent stages, which are closer to the market, by providing access to the larger European security market, promoting European standardisation and certification efforts, while at the same time ensuring competition.
  - To address **short-term innovation** (compared to research) needs, 'functional' DGs with security responsibility should complement the funding of security research under H2020. For example DGs ECHO, CNECT and SANTE could provide the necessary funds to tackle short-term needs in their areas. Such a mechanism would be analogous to the 'specialisation' of funding existing in many Member States and many stakeholders would be familiar with the 'division of labour'.
  - **Information** about national security research programmes, as well as the different funding possibilities provided by other DGs such as DGs RTD, CNECT and MARE should be systematically collated and regularly updated. Stakeholders are usually not aware of the multiple opportunities to receive (complementary) funding. At EU level, there are other sources of funding for security research and innovation, which, while complementing the FP7 Security Research Actions, are not known to many stakeholders. For example structural and social funds provide funding opportunities for the procurement of innovative solution in the security area. Stakeholders have to be made more aware of the existence of such funding mechanisms outside the FP7.

Appendix G Summary of the stakeholder workshop

Summary of the focus group (stakeholder) workshop on preliminary results of the final evaluation of the FP7 Security Research Programme

Brussels on 29th April 2015

Background and objectives

This note summarises the results of a focus group workshop that was held as part of the final evaluation of the FP7 Security Research Programme. The one-day event took place on 29th April 2015, with invited experts and the project team in attendance.

The purpose of the workshop was to seek input from the assembled experts on the **preliminary findings and conclusions of the evaluation**, and in particular with regard to the project team's assessment of the relevance, efficiency, effectiveness and impact of the Security Research Programme. The team also wished to discuss with the group possible ways in which to tackle challenges in the future, e.g. how to enhance the valorisation of FP7 projects, or how to strengthen end-user engagement.

As such, individuals with a *programme*-level view of the FP7 Security Research Actions were invited to participate.

Participants

The workshop brought together **21 participants from 11 Member States** and 4 European institutions. They represented national security authorities, research organisations and public funding bodies, as well as companies in the security sector (end-users).

While approximately half of those participating had already contributed to the evaluation through surveys or stakeholder interviews, the remainder were being consulted in relation to the evaluation for the first time. In this way the discussion was intended to provide an opportunity for reflection on the preliminary results as much as to provide additional perspectives to the analysis of the project team.

Approach

During the workshop participants were invited to **discuss** the preliminary results and recommendations proposed by the project team. Both had been summarised in an input paper circulated to all attendees prior to the event, but these were also reintroduced through a series of presentations given during the day.

Discussion of preliminary findings

Participants generally endorsed the main findings of the evaluation as set out in the input paper, with some critical reflection on specific issues and further points and ideas for consideration. Some of the key issues arising were:

Rationale

Discussions of the rationale and relevance of the programme focused on whether it was addressed to the right mix of issues and areas. In particular:

- It was pointed out that the general **objectives** of the FP7 programme might be understood as contradictory, since they focus both on increasing security for all and on industrial competitiveness at the same time.

- A majority of participants agreed that the programme covered all significant **areas** of security and insisted that it is of continued importance to cover both technology-oriented projects and non technology-oriented projects – including social science projects. To ensure such an orientation, it was felt that the composition of the agenda-setting committees should be made more diverse.
- It was noted that calls are sometimes related to **pressing and emerging issues**, but that the entire process to: (i) identify a problem, (ii) launch a call for proposals, and (iii) select projects, could be very long, with the risk that, in the end, outputs are no longer relevant to stakeholders or to solving pertinent issues.

Implementation

Discussions relating to the implementation of the Security Research Actions centred around four main issues: the engagement of the right actors, the application of the right instruments, the support to maximise project success and impact, and the internal collaboration of different parts of the EC.

- There was a general sense that the programme could have done more to reach and engage the right **actors**. For example, some participants viewed it as desirable and useful to have more citizens involved, as well as EU authorities and social sciences and humanities experts. Others disagreed. Moreover, project results were judged not to be sufficiently visible to those people and organisations that could apply them or make other use of them.
- It was noted (positively) that the programme was innovative with regard to new ways of funding R&D, i.e. through the use of new **instruments**. However, these brought with them new types of challenges. Cross cutting missions were seen as important, as "catch-all fields" and for tackling new types of threats. However, there was felt to be insufficient contact and cross-fertilisation between projects that were addressing related or similar topics.
- There was general agreement that the **dissemination** of project results could be improved. One issue is that dissemination currently tends to be done by each individual participant, rather than at project or programme level. Another issue relates to the challenges related to classified information. Finally, some participants advised the study team to make a clearer distinction between the dissemination (telling people about the results) and exploitation (implementing the results) of research results and to consider ways to promote both ways of **valorisation**. This was perhaps the one issue where every delegate was in strong agreement and together asked that the evaluation team make sure to include a recommendation encouraging the Commission to devote substantially more attention to this aspect going forwards.
- Finally, participants were under the impression that the **internal cooperation** between different parts of the EC could be improved. On the one hand, other DGs with a security brief are not felt to have been sufficiently involved in setting the agenda for the Security programme, or in then following relevant projects. On the other hand, the EC and REA face the challenge of ensuring the development of an effective organisational capability to formulate work programmes, manage projects, and to communicate results. Some participants were under the impression that some project managers from REA knew too little about the content of the projects they were managing, and that they did not always attend meetings in which a project team presented results. It was also felt that exchange between the REA and the Commission could be improved.

Achievements

At the time of this evaluation, a large number of projects are still on-going. Moreover, the nature of much Security research implies that it is likely to take several years from now before results will have a visible impact in the wider security landscape and marketplace. Consequently, and given this was the first security research programme, it was considered worthwhile to review the achievements of the FP7 Security Research Actions again in the future to better understand impacts and impact pathways (even though this may be outside the conventional programme evaluation cycle).

There was, though, a general sense that the programme has already yielded significant achievements. Participants however highlight a small number of issues:

- On a positive note, it was felt that the Security Research Actions may have a number of indirect impacts that have not been within scope for the evaluation, but have nevertheless strengthened security research and industry. Participants also regarded the FP7 Security Research Actions as a significant success in developing EU-wide security research of good quality. In particular, they found that the programme **shaped the landscape** of security research, industry and end-users, leading to new links in Member States as much as across the EU. For example in Ireland, the FP7 Security Research Actions have allowed for the creation of the Irish Security Research Network, which includes about 950 academics, SMEs, LEs, civil/public servants, end-users, civil society, etc.
- As for the **involvement of SMEs,** participants critically discussed the claim that the Security Research Actions have been a particular success in this regard. Several participants remarked that the FP7 Security Research programme, with its long project duration and large number of partners, seems not to be specifically well designed for SMEs, but rather for the involvement of larger companies. One participant also observed that many SMEs participating in projects were assigned to management and dissemination tasks and other rather non-innovative functions. Moreover, there is also an issue with confidentiality concerning research results, where SMEs and other end-users have experienced difficulties in getting access to project results.
- In addition, it would be helpful to have one point of information for getting an overview of what research activities have been funded in the different areas of the programme, and what has been achieved, on a European as well as a national level. A publicly accessible **repository** of all the outputs produced during each project was considered by many participants as a useful means to help with the dissemination and exploitation of results. The Cordis website was not seen to be sufficient in this regard.

EU value added

With regard to the European value added of the FP7 Security Research Actions, participants raised the following main points:

- **European added value** was considered particularly evident in terms of the support for transnational co-operation, the complete additionality of a Security research programme for many MS, and improvement in researcher quality achieved during projects. The programme also allows for the identification of best practices, thus improving the overall quality of projects. This was felt to have been especially clear European added value when end-users have been actively involved in project work.
- The programme is felt to be **relevant** for many stakeholders, both in the small number of MS that have a security related R&D programme, and in those that don't. Participants were of the view that the programme was complementary to what is funded at national level, which was indicated by a lot of exchanges between national stakeholders and the EC.

Discussion of conclusions and recommendations

Participants largely endorsed the preliminary conclusions and recommendations presented in the input paper. Several qualifications and details were added to individual recommendations, which the team has noted. Here, instead, focus is on outlining the *additional* recommendations that were made by participants.

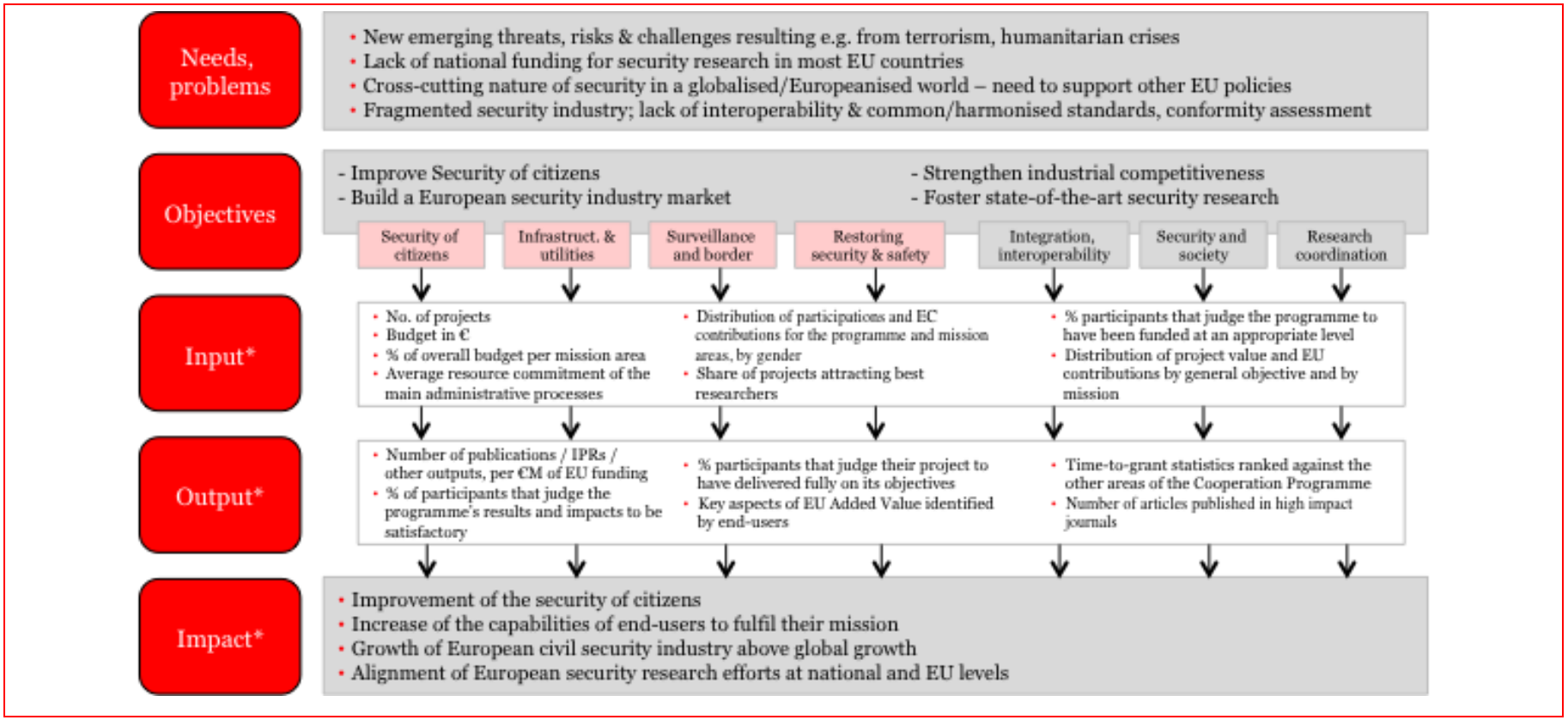
During the discussion **participants suggested the following measures** to improve the Security Research Actions:

- Access to project **outputs** should be improved through a proper archive scheme. The EC should also play a greater role in encouraging and supporting the dissemination and exploitation of results.
- There would be value in more programme-level **dissemination** activities, perhaps including clustering events built around groups of similar projects

- There should be a dedicated budget for the independent **testing** of results and for certification.
- The Commission should maintain an interest in projects / project results following conclusion of the work, in order to press partners to pursue the application of results (rather than moving on to the next grant) and also look at other follow-on support measures to facilitate take-up and exploitation (valorisation)
- As **certification and/or standardisation** activities are very efficient ways to create markets, there need to be stronger connections between Security research projects and standardisation bodies.
- The programme should be made more **SME-friendly**: at the moment most projects are very large, but the REA tends not to want SMEs to run larger projects because they do not have the internal capacity or experience and tend to run into difficulties. The situation could be improved through the use of new instruments, such as pre-commercial procurement, or the SME instrument of H2020/COSME.
- **Citizens and societal groups**, as well as end-users should be more engaged in the programme. The EC should think in particular about ways to engage and educate the very diverse range of potential end users, and to make sure project participants interact with end-users, so as to improve the value and quality of projects.
- A certain proportion of security research projects should be required to finish within a **2-year time frame**. This should be applied in particular to topics at TRL 6 or above. Such a short time frame would allow for in-programme feedback, adjusting for what works and what does not work. Moreover, it would set an incentive to build on the research results of finished projects and add further dynamic to the valorisation of results.
- The idea of a security-related **European Innovation Partnership** was broadly welcomed as an interesting possibility by which end-users, industry and society might be brought together to both direct development efforts and take-up results where appropriate. The European security community would benefit from the greater flexibility of these instruments too, inasmuch as they may be able to support smaller research projects alongside larger demonstrations, but possibly also proof of concept activities or studies
- **Industry** delegates were keen to emphasise that businesses will really only wish to participate where the calls for proposals / projects are judged likely to provide a basis for developing future products and services and addressing markets directly

Appendix H Intervention logic

Figure 37: Intervention logic



Source: Technopolis

NB-02-14-003-EN-N