


D.2.3 Lessons learned about the effectiveness of the uptake of research results

Deliverable submitted in November 2012 (M6) in fulfilment of the requirements of the FP7 project, ETTIS – European security trends and threats in society

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 285593.

	ETTIS Coordinator: Peace Research Institute Oslo (PRIO)	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.ettis-project.eu
---	---	--	--	--

Project Acronym	ETTIS
Project full title	European security trends and threats in society
Website	www.ettisproject.eu; www.ettis-project.eu
Grant Agreement #	285593
Funding Scheme	FP7-SEC-2011-1 (Collaborative Project)
Deliverable:	D2.3
Title:	Report on lessons learned
Due date:	30 November 2012
Actual submission date:	Extended 31 January 2013
Lead contractor for this deliverable:	Trilateral Research & Consulting LLP
Contact:	Monica Lagazio Monica.lagazio@trilateralresearch.com
Dissemination Level:	PU- Summary RE- Appendix

	LEAD	CONTRIBUTORS
AUTHORS	Monica Lagazio, Trilateral Research and Consulting	Matthias Weber, Joachim Klerx and Katharina Jarmai, Austrian Institute for Technology; Sonja Grigoleit, Fraunhofer INT.
REVIEWERS	Timo Leimbach, Fraunhofer ISI; Peter Burgess, Peace Research Institute.	

1 EXECUTIVE SUMMARY.....	4
2 INTRODUCTION.....	7
2.1 Objectives.....	7
2.2 Approach.....	8
2.3 Key general dimensions of security.....	9
3 ANALYSIS OF EU AND NATIONAL PROJECTS.....	9
3.1 Types and trends for decision-making-support methodologies.....	10
3.2 Principal barriers and limitations to the uptake of research results.....	14
3.2.1 Institutional-organisational barriers and limitations.....	18
3.2.2 Financial barriers and limitations.....	19
3.2.3 Cultural barriers and limitations.....	20
3.2.4 Technological barriers and limitations.....	21
3.2.5 Research barriers and limitations.....	21
3.3 Recommendations for the enhancement of the uptake of research results.....	21
4 ANNEX 1: SECURITY TAXONOMY.....	25

1 EXECUTIVE SUMMARY

This document provides an in-depth analysis of completed foresight and other relevant security projects, undertaken both in Europe and beyond, in relation to key insights on decision-support methodologies for security, barriers and limitation to the uptake of research results, and possible recommendations to enhance the uptake of research results by security end-users. The main objectives of the analysis are to ensure that ETTIS work builds on the research and findings of others and to achieve further uptake of ETTIS research results by applying the learning from previous projects. Given time and resource constraints, the analysis is based on a sample of projects illustrating several dimensions of security: physical, political, social, economic and cultural, environmental and radical uncertainty, cyber and information.

We have structured the investigation around three main areas: the type of methodologies and tools that have been used and/or developed for instructing and supporting decision-making in security contexts; the principal barriers and limitations to the uptake of the research results that research teams, doing research in security, have experienced; and recommendations that could be taken to enhance the uptake of research results by security end-users. The following section is an executive summary of the most important findings of the analysis.

Key insights in decision-making-support methodologies

- The most popular general category of decision-making-support methodologies is *risk and foresight approaches* in almost all the security dimensions, while *monitoring and surveillance tools for early warning* is the principal category in the physical dimension.
- The majority of the projects put forward and/or use a combination of decision-making tools to support decision-making process. This underlines that the complex and changing nature of nowadays security environment requires several, innovative and adaptive decision-making tools to support decisions from the strategic to the operational level.
- The majority of selected projects have developed and/or used decision-making-support methodologies designed to instructing and facilitating the decision-making process for policy-makers, regulatory, administrative and enforcement agencies, operating both internationally and nationally. This underlines a traditional concern with the state, as the main actor and active user of decision-making-support tools in security.
- Within the physical dimension, decision-making methodologies and tools are centred on the needs of enforcement agencies. Strengthening monitoring and surveillance capabilities of enforcement agencies for early warning is the focus of several projects.
- Within the most popular category, *risk and foresight approaches*, the majority of approaches make use of traditional trends analyses, which are difficult to replicate and/or adapt in different security contexts. Therefore, the projects tend to provide somehow static assessments of risks and possible futures, using established risk and foresight methods.

Key insights in barriers and limitations to the uptake of research results

- Similar, specific barriers and limitations to the uptake of the research have been experienced by researchers with different levels of security end-users.
- The most popular categories of barriers experienced with all the security end-users are: *Cultural* and *institutional-organisational*. *Financial* and *research limitation* type of barriers are also important but less prominent, while *technological barriers* appear to

have little relevance with both states and private companies and almost no relevance at all with society.

- Public administration and industry are still seen as the main “up-taker” of research results with society and individuals taking a back seat. The perception appears to be that society and individuals will indirectly uptake the results of research projects if public administration and industry do so.
- National research teams appear to be in general more positive towards the impact of their research results than European teams, irrespectively to the type of projects (i.e., new technological developments or strategic analyses) and/or security dimensions that they are addressing. This is because national teams tend to have closer relationships with the main stakeholders, who are supposed to use or implement their research outcomes.
- Within the institutional-organisational category, some barriers appear to dominate the uptake of research results. The most common institutional-organisational barriers and limitations, experienced with all the security end-users, are: the lack of alignment of the research project with stakeholders ‘overall priorities, regulatory constrains and legal and organisational structure of FP7 programmes. Lack of established mechanisms for translating end-users’ needs into technical requirements and service is also important when dealing with technology programmes directed towards public and industry end-users. Lack of mechanisms/feedback to monitor how strategic insights are incorporated into decision making is another important and more specific barrier related to strategic type of projects directed towards the state.
- Within the cultural barriers and limitations, organisational culture is the most mentioned constrain for all security end-users (i.e., state, company and society), security dimensions and type of projects (i.e., technological and strategic programmes), followed by lack of understanding /awareness of research topics, results and processes, and lack of trust in research results and researchers.
- Within financial barriers, lack of post-research budget for implementation and go-to-market activities is the most mentioned constrain in relation state and industry actors, while lack of budget to disseminate and promote research results is critical when dealing with societal actors.
- Within research limitations, lack of real data to validate new technological developments and/or lack of research focus on business opportunity is especially relevant when dealing with the uptake of technology research by industry players. Lack of an operationalisation and implementation component within the research output is more important for strategic type of projects directed towards all the security end-users.
- Technological constrains (e.g., technological infancy and need for further testing) are hardly mentioned by any of the surveyed projects and only by technology programmes.

Key recommendations to enhance the uptake of research results

- Based on our analysis on barriers and limitations to the uptake of research results and additional insights from the survey and interviews, we have developed key cross-cutting recommendations in the form of four general observations and six specific insights.
 - *Observation 1:* Decision-support in the area of security has become more complex and raises new requirements for both providers and users of decision support.
 - *Observation 2:* It is increasingly recognised that due to the more complex security picture, more sophisticated foresight methods and risk analyses are

needed as a basis for security strategy and operations. These foresight and risk assessment tools need also to become more operational and geared towards specific needs of security-end user.

- *Observation 3:* The thus far dominant state-centred approach to security is increasingly challenged, while opening up opportunities for introducing novel and innovative concepts for tackling security issues into the public and policy debates.
- *Observation 4:* Early warning methods and tools have significantly evolved in recent years due to new developments in surveillance technologies. Consequently, there is a need to strike the right balance, within security research programmes, among security, trust, democratic rights and the new opportunities offered by these new emerging technologies in order to build more resilient societies.
- *Insight 1:* The early and right form of involvement of potential end- users in research and development activities needs to be given a more prominent role in security research. This is crucial for successfully making the step from testing to widespread implementation, from pilots to commercialisation.
- *Insight 2:* The State, and also industry, has a key role to play as pacemakers and lead agents in the adoption of new technological as well as non-technological approaches to tackling security issues. The ability to play that role needs to be fostered.
- *Insight 3:* The cultural (and sometimes institutional-organisational) barriers to adoption need to be taken much more seriously. Conservatism and risk-averseness are well established virtues in the security field, but they hinder the introduction of new promising solutions and insights.
- *Insight 4:* The diversity and rigidity of security-related regulations in Europe are too high. They prevent new security technologies and options to be adopted quickly.
- *Insight 5:* There is a conceptual issue that contributes to slowing down the uptake of new security solutions, which consists of the perseverance of established mental frameworks and way of thinking about security issues. Opening up mindsets is thus a major issue for accelerating the uptake of research results, and it should be given a more prominent role in security research.
- *Insight 6:* EU-funded security research projects are confronted with a number of specific barriers to uptake. Both the practice and the regulations of EU security programmes need to be adjusted in order to make the outcomes more attractive to potential users of research results.

2 INTRODUCTION

This document provides an integrated overview of a subset of completed foresights and other relevant security projects, undertaken both in Europe and beyond. The aim of the analysis is to identify

- the key characteristics emerging from existing security research projects and programmes in relation to: the type of methodologies and tools that have been used and/or developed for instructing and supporting decision-making in security contexts;

- the principal barriers and limitations to the uptake of the research results and recommendations that research teams, doing research in security, have experienced; and
- the possible actions that could be taken to enhance the uptake of research results by security end-users.

The analysis in the report is closely integrated with other ETTIS work packages. Building on the finding of WP1, “Sources and dimensions of security”, this report has endorsed a broad and holistic approach to security, which takes into consideration the nexus and complexity of both the external and internal dimension of security, as well as the views of different levels of end-users, ranging from intergovernmental organisations, states, companies, societies and individuals. The report has also drawn from the extensive stocktaking exercise and the findings on the identified key security threats, user needs and security solutions put forward in the previous work package reports (WP2.1 and WP2.2). Finally, the findings of this report will feed into the subsequent work of the ETTIS consortium. Specifically, the consortium will use the findings in WP3 to integrate the lessons learned on uptake of research results into the development of the ETTIS own decision-making methodologies and tools for security, in particular to better gear them to the needs of potential users, and in WP7 to refine ETTIS communication and uptake strategy on the basis of stakeholder and user needs. Furthermore, this report is in line with the overall methodological framework established in WP3.

We have articulated the structure of this report around two sections. The first section provides the summarised analysis of the key findings emerging from the in-depth investigation of a subset of projects. The findings focus on: (1) the summary of the key categories and types of methodologies and tools that have been used and/or developed for instructing and supporting decision-making in different security contexts; (2) the summary of the types and categories of principal barriers and limitations to the uptake of security research results, experienced within the selected projects; and (3) the summary of the types and categories of possible improvements that could be undertaken for enhancing the uptake of security research by security end-users. The second section, which for confidentiality and privacy reasons is restricted to the members of the consortium, presents a detailed analysis of the individual research projects along the same structure (decision making methodologies and tools, barriers and limitations to the uptake of security research, improvements for research uptake).

2.1 OBJECTIVES

The key objectives of the in-depth analysis of the existing research projects are: (1) to provide an overview of the key findings of previously undertaken security research projects and programmes in Europe and beyond; (2) to facilitate and enable research exchange and utilisation of previous research results; to enable learning from previous and relevant research works; (3) to ensure that the ETTIS work builds on the analysis and findings of others; and (4) finally, to achieve further contextualisation and quality assurance of ETTIS final research results.

Indeed, ETTIS aims both to build on the findings and experiences of other EU-funded projects and to consider the security perspectives of third countries and other agencies and organisations. This will lead to robust and encompassing research outcomes, while avoiding waste of resources and/or redundant work.

2.2 APPROACH

In order to identify the key lessons learned about decision-support system and effectiveness of the uptake of security research undertaken in Europe and beyond, we have analysed a subsample of projects, drawn from the extensive stocktaking project list and compiled with information provided by consortium partners and desktop research. The reader should view this analysis in the context of the ETTIS project and not as a comprehensive analysis of the projects and/or their activities.

Initially, we have compiled an extensive project list of 420 projects from a wide range of security programmes, representing the diverse dimensions of security (see Table 1), and different funding organisations (e.g., EU, think tanks, other Intergovernmental Organisations (IGOs), Non-Governmental Organisations (NGOs), research institutions, academia). Given the huge amount of data and the resource limitations, it was impractical to perform an in-depth analysis of the extensive list of projects. Therefore, the consortium identified a subsample of 32 projects, based on a purposive sampling approach. We have attempted to ensure that the selected 32 projects represent the diverse dimensions and categories of security identified in the security taxonomy (Figure 1), while providing some differentiation in relation to funding agencies and type of security projects (i.e. both projects focusing on technological developments and strategic analyses). The sample covers the main practical dimensions and categories of security (physical, political, socio-economic, cultural, environmental, radical uncertainty, and information and cyber), which the partners have identified as important based on WP2.2 and WP1.2 results. It also includes a sample of projects funded by different FP7 programmes, other IGOs, NGOs, third countries, think tanks and research institutions. Although the partners sought to select ‘the best’ or “most interesting” sample, we acknowledge, that out of necessity, we might have excluded some projects which may have had different features and included some which finally turned out to be less relevant than initially expected.

We have then analysed the 32 projects following the same pattern of analysis and inquiry that mirrors the information needs of subsequent work packages. Our analysis has been directed by the following questions:

1. Which kinds of methodologies have been used for instructing and supporting decision making?
2. Which types of barriers and limitations to the uptake of the research have been experienced?
3. How can the uptake of research results by security users be enhanced?

The analysis relies on both primary data, collected via a survey, and a systematic investigation of secondary sources. We will seek to validate the report’s findings in a workshop with the ETTIS reflection group, policy-makers and stakeholders.

2.3 KEY GENERAL DIMENSIONS OF SECURITY

Based on the taxonomy developed in WP2.2, we have used the same security dimensions for categorising the projects.¹ WP2.2 has developed a useful and actionable list of security dimensions, which serve both as guidance and as a checklist for the type of dimensions considered in societal security policy-making. It also proves useful in this work package that tries to identify methodologies to support decision-making, barriers and limitations to the uptake of research results and possible enhancements to research uptake. Our taxonomy is based on the seven dimensions of security identified in WP2.2 analysis: physical, political, socio-economic, cultural, environmental, radical uncertainty, and information and cyber. To provide a more granular and multi-level picture as well as elaborate the meaning and actual reference of security and what precisely needs to be secured these seven dimensions were cross referenced with the following five types of security actors: intergovernmental organisations, states, private companies, civil society, and individual households (see Table 4 in the annex). By applying this framework, we can try to identify a few differences and/or similarities in the sample that could lead to interesting insights on uptake of research, which security researchers have experienced with different levels of security end-users. As a result, we can provide more targeted and focused insights aimed at reflecting on interdependencies, diversity and multidimensional aspects of security research in Europe, specifically in relation to decision-support tools and methodologies, used in security decision-making, as well as multi-actor-level recommendations in which research uptake in societal security could be enhanced.

3 ANALYSIS OF EU AND NATIONAL PROJECTS

This section presents the key findings of the analysis of the 32 research projects and programmes that were selected for the in-depth investigation. We have structured the section into three parts:

1. summary of the key types of methodologies to support decision-making in security, which the research projects have used and/or developed;
2. summary of the key categories of barriers and limitations to the uptake of research, which the researchers projects have faced; and
3. summary of the key recommendations for enhancing the uptake of research results by security end-users, with special focus on industry and public administration.

The Table 1 lists the selected 32 projects by security dimensions and type of funding received.

	List of 32 projects	Funding/organisations
	<i>Physical dimension</i>	
1	AMASS	FP7
2	INFRA	FP7

¹ See ETTIS - European Trends and Threats in Society, Seventh Framework Programme European Union, *Report on Research Approaches and Results (WP2.2)*.

3	ACRIMAS	FP7
4	WiMA ² S	FP7
5	TALOS	FP7
6	UNCOSS	FP7
7	CBRNemap	FP7
8	EURACOM	FP7
9	COCAE	FP7
10	BeSeCu	FP7
<i>Political, economic, cultural and social dimension</i>		
11	55 trends	National (US government)
12	EUSECON	FP7
13	Muslims in Europe	National (US government)
14	Countering Terrorism	Regional, IGO (Asia)
15	Global risks from 2008 to 2012	International, IGO
16	SAFIRE	FP7
17	RE-DESIGN	National-academia
<i>Environmental and radical uncertainties dimension</i>		
18	SECURENV	FP7
19	EFONET	FP7
20	Issue brief No. 4: the resource scarcity nexus	National-think tank and academia
21	SECUREAU	FP7
22	International crisis group: Climate change and conflict	International-think tank
<i>Information and cyber dimension</i>		
23	ICE	FP7
24	NOTZERT	National-academia
25	ESCoRTS	FP7
26	CuteForce Analyser	National-academia
<i>All dimensions</i>		
27	FORESEC	FP7
28	Studies in African Studies	National-think tank
29	Global trends 2025	National-(US government)
30	ESRIF	FP7
31	Strong in the 21st century	National-academia
32	Oxford research group sustainable security programme	NGO

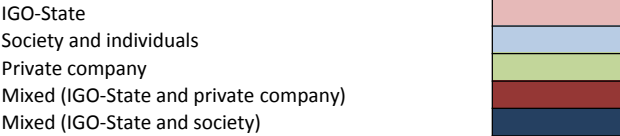
Table 1 Sample of Research Projects

3.1 TYPES AND TRENDS FOR DECISION-MAKING-SUPPORT METHODOLOGIES

The examination of methodologies and tools that have been used for instructing and supporting decision making (“intelligent methods”) across the 32 projects has provided some interesting results. In addition to confirming a number of more or less well-known facts, the overview also yields a series of interesting insights that the ETTIS partners can build on during the remainder of this project. Below, we present a synthesis of the most important findings and key trends emerging from the in-depth analysis.

We have used the security dimensions and categories of actors, detailed in Table 1 in Section 2.3, to organise the findings from the individual projects. We have constructed a list of key trends in decision-making-support tools and methodologies within security by clustering the types of tools and methodologies found in the 32 projects following the security dimensions detailed in Section 2.3. Furthermore, we have also tried to differentiate to which type of security end-users these decision-support-methodologies have been directed. Based on the actors identified in Table 1, we have focused on three types of security end-users: IGO and state, private company, and society and individuals. The IGO and state type refers to policy-

makers, regulatory, administrative and enforcement agencies, operating both internationally and nationally. Private company regards private company actors and providers. The society and individual refers to civil organisations and civil operators but also single individuals. We have also counted how many projects identify the same methodology trend in order to provide an indication of the popularity or importance of the trend.² Table 2 details the result of the clustering by key security dimensions and end-users types.



Dimension of Security	Decision-making- support methodologies	N. of Projects
Physical	Monitoring and surveillance tools for early warning	6
	Tools for early detection, surveillance and monitoring for border control including sea sensor systems for early detection and location of vehicles (e.g. small and midsize vessels)	5
	unmanned vehicles for surveillance	1
	sensor systems for detection of dangerous material (e.g., explosive underwater, radioactive sources)	2
	Sensor monitoring systems to support crisis management at critical infrastructures	1
	Risk and foresight approaches	3
	Foresight scenario/simulation tools (e.g. to identify critical future areas of research in crisis management)	2
	Risk management methodologies/principles (e.g., f or energy sector).	1
	Crisis management	2
	Integrated communication and data sharing systems (to support and communicate decisions)	1
	Evacuation methodologies/principles	1
	Policy planning	1
Contingency planning methodologies/principles (e.g., f or energy sector).	1	
Political-Socio-Economic - Cultural	Risk and foresight approaches	8
	Traditional trend analyses/studies	3
	Analytical risk tools (e.g., risk models and databases)	2
	Risk guidelines (e.g., risk management principles and standards)	1
	Impact diagnostics tools (e.g., visualisation tools)	1
	Foresight scenario analyses /tools	1
	Policy planning	6
	Development of high level recommendations and policy principles	5
	Decision support frameworks (e.g., for building resilient urban infrastructures against terrorism)	1
Environmental & Radical Uncertainty	Monitoring for early warning	1
	Sensor systems for early detection of environmental contamination (e.g., water contamination)	1
	Risk and foresight approaches	5
	Traditional trend analyses/studies	2
	Foresight scenario analyses /tools (e.g., predictive models for energy, spread of contaminated water)	3
	Policy planning	5
	Development of high level recommendations and policy principles	3
	Sector specific action/mitigation plans (e.g. . for energy efficiency and technology plans)	2
	Crisis management	1
Crisis management principles/guidelines to respond to environmental disasters (e.g., hurricane season)	1	
Cyber	Crisis management	1
	Emergency scenario simulation tools (e.g. to plan responses after cyber attacks)	1
	Policy planning	2
	General SWOT analysis (e.g., to identify R&D developments)	1
	Market analyses	1

² The result of the popularity or importance assessment should be taken as directional. This is because the results are based on 32 projects.

All	Risk and foresight approaches	10
	Delphi analyses	1
	Traditional trend analyses/studies	4
	Risk guidelines (e.g., risk management principles and standards)	1
	Analytical risk tools (e.g., predictive models)	1
	Foresight scenario analyses /tools	3
	Policy planning	5
	Development of high level recommendations and policy principles	4
	General scenario planning tools	1
	Monitoring for early warning	1
	Discourse and information monitoring tools (e.g., to identify new drivers of future and early warning indicators)	1
	Crisis management	1
	General crisis management guidelines /principles (e.g. in post-conflict phase)	1

Table 2 Decision-making support trends in the security projects

This exercise resulted in a set of four categories of methodology trends (in grey in the table) for the physical dimension, two for the political-socio-economic and cultural dimension, four for the environmental and radical uncertainty dimension, two for the cyber and information dimension and four for the overall dimension³. The most popular general category of decision-making-support methodologies appears to be *risk and foresight approaches* in almost all the dimensions, while *monitoring and surveillance tools for early warning* is the principal category in the physical dimension.⁴

In relation to key findings emerging from the analysis of the selected single projects, some interesting insights have emerged. First, the majority of the projects tend to put forward and/or use a combination of decision-making tools to support decision-making process. This underlines that the complex and changing nature of nowadays security environment requires several, innovative and adaptive decision-making tools and methodologies providing autonomous and intelligent planning and decision-support from the strategic to the operational level.

A second key trend appears to be the consistent focus on the IGO and state level of security. The majority of selected projects and research activities have developed and/or used decision-making-support methodologies designed to instructing and facilitating the decision-making process for policy-makers, regulatory, administrative and enforcement agencies, operating both internationally and nationally. Only few projects that tend to be European funded and address the physical dimension of security have directed their attention to support decision-making for civil operators and/or industry players.⁵ These projects have developed intelligent tools to support operational decision-making. These intelligent tools enable informed and fast decisions in the “response” and “recovery” phase of *crisis management* by opening up new sources of information (e.g. by advanced sensor systems) and exchanging information in near real-time⁶ as well as allow the identification of sector specific risks and contingency plans by putting forward coherent and integrated risk management and contingency planning principles and processes.⁷ Although the traditional concern with state, as the main actor in security, appears to be still dominant in relation to research and development of intelligent decision-making tools, these few projects underline the growing acceptance, at the European level, of a

³ The overall dimension includes projects that cover all security dimensions.

⁴ Given the small number of surveyed projects, this count is only directional.

⁵ See in the appendix: “INFRA”, “EURACOM” and “BeSeCu” projects.

⁶ See <http://www.infra-fp7.com/>.

⁷ See <http://www.eos-eu.com/?Page=euracom>.

comprehensive approach to security, which takes into consideration the participation of multiple users in the security enterprise and therefore the need to support them in their decision-making process.

Third, within the physical dimension, decision-making methodologies and tools are centred on the needs of enforcement agencies. This is especially evident in more recent programmes. Strengthening monitoring and surveillance capabilities of enforcement agencies for early warning is the focus of several projects. This has translated into developing *early warning, detection and monitoring tools*, ranging from sophisticated sensors to unmanned vehicles for surveillance, which can be applied in several security contexts, such as critical infrastructures protection and border control, and could help guide decisions and interventions by collecting and assessing data in pre-and-post harmful event phase.⁸

Four, the general category of risk and foresight methodologies appears to be the most important across almost all the security dimensions. Several of the analysed projects have used or developed risk and scenario tools to direct decision-making.⁹ This is in line with the idea that security end-users will make better decisions when these are based on a sound risk management approach, which contains elements of foresight to deal with risk scenarios that change over time. However, several risk and foresight approaches appear to make use of traditional qualitative trends analyses, which are difficult to replicate and/or adapt in different security contexts. This is especially evident in national projects and programmes that tend to apply trend extrapolation and expert polling.¹⁰ Therefore, the projects tend to provide somehow static assessments of risks and possible futures, using established risk and foresight methods. *The same can be said for policy planning methodologies. Although several projects strive to strengthen the strategic decision-making and policy-planning capabilities of policy-makers, both at the national and European levels, in areas such as energy, crime and terrorism, environmental protection and degradation, this often translates into providing high level policy recommendations and developing policy principles to be applied in general or specific policy areas.*¹¹ Similarly to the risk and foresight category, the policy planning exercise sometimes becomes “developing general or specific guidelines and /or recommendations” rather than providing adaptive tools and methodologies that decision makers can use to evaluate the effects of potential decisions and therefore elaborate efficient solutions for a variety of security contexts.

⁸ This is particularly evident in projects such as “AMASS” and “WiMA²S”, which focus on border control. For more details see appendix.

⁹ In particular “55 Trends”, “Global Risks”, “Issue Brief N.4”, “FORESEC”, “Global Trends 2025” and “ESRIF” combine risk and scenario methodologies. See appendix.

¹⁰ “55 Trends” is a typical example of this type of projects. See appendix for more details.

¹¹ For example of projects focusing on policy recommendations see the following projects in the appendix : “55 Trends”, “Muslims in Europe”, “Countering Terrorism”, “SECURENV”, “EFONET”, “International Crisis Group”, “FORESEC”, “Studies in Africa Security”, “Global Trends 2025”, “ESRIF”, “Strong in the 21st Century”, and “Oxford Research Group”.

Finally, little development of decision-support-making methodologies seems to happen within cyber security. This might be due to the greater need within the domain for technological solutions, addressing advances in cryptographic techniques, operating systems, domain name and social networking security, which take priority on the development of decision-support tools.

3.2 PRINCIPAL BARRIERS AND LIMITATIONS TO THE UPTAKE OF RESEARCH RESULTS

In this section we have constructed a list of principal barriers and limitations that the projects surveyed have experienced in relation to the uptake of their research results (see Table 3). Based on the actors identified in the security taxonomy (see table in the annex), we have focused on three types of security end-users and use these three types to organise the findings of the single project analysis: IGO and state, private company, and society and individual. The IGO and state refers to policy-makers, regulatory, administrative and enforcement agencies, operating both internationally and nationally. The society and individual type refers to civil protection authorities, civil organisations and civil operators but also single individuals. Private company regards private company actors and providers. As for the decision-making support methodologies analysis, we have counted how many projects identify the same barriers and limitations in order to provide an indication of the popularity or importance of the identified barrier and/or limit.

This exercise has resulted in a set of five key types of barriers and limitations, experienced in relation to uptake of research results, when dealing with states, IGOs and private companies. Four types of barriers and limitations were instead found when dealing with society and individuals. The most popular categories of barriers experienced with all the security end-users are: *Cultural* and *institutional-organisational*. *Financial* and *research* limitation type of barriers are also important but less prominent, while *technological barriers* appear to have little relevance with both states and private companies and almost no relevance at all with society. Finally, the table’s summary also indicates that similar, specific barriers and limitations to the uptake of the research have been experienced by researchers with different types of security end-users.

Type	Barriers/Limitations to the uptake of research results	N. of Projects 26 ¹²
IGOs/s tate	Institutional-Organisational	16
	Legal and organisational structure of FP7 programmes (e.g., lack of enforceability and flexibility,	4

¹² The same project may deal with several barriers at different types of security end-users. For instance a project may have experienced both cultural and institutional-organisational barriers in relation to state and industry actors. Furthermore, in relation to the cultural type of barriers, the project may have experienced several, specific barriers simultaneously, such as lack of understanding/awareness of research topics and lack of availability of and accessibility to relevant stakeholders. Since the projects could deal with multiple type of barriers and specific barriers, the total frequency for each main barrier category does not equate with the summation of the specific barrier frequency.

	lack of policy focus , lack of reference to EU market procurement) Regulatory constrains (e.g., rigid regulations on the use of new technologies, different regulations across EU , security sensitivity, artificial divides between external and internal security) Lack of clear guidance and objectives from stakeholders/ lack of established mechanisms for translating end-users' needs into technical requirements and service specifications Complex and unco-ordinated stakeholder structure (e.g., too many organisations at national and European levels) Organisational silos and different internal organisational priorities Lack of mechanisms/feedback to monitor how strategic insights are incorporated into decision making Procurement processes Lack of institutional mechanisms for research transfer (e.g., implementation programmes) Lack of long-term political stability and therefore log-term planning Lack of alignment with organisational overall priorities , or new priorities, and processes (this includes processes focused on quick decisions/wins and business as usual)	6 2 1 4 2 1 1 1 1 8
	Financial Lack of budget to disseminate and promote research results (above all in post-research phase) Lack of post-research budget for implementation and go- to-market (e.g., to support development from prototype to product , commercialisation of research results, implementation at national level and for specific contexts, etc.) Lack of budget for field work	3 5 1
	Cultural (including awareness-trust) Lack of understanding /awareness of research topics, results and processes (e.g., how does this result apply to me?) Lack of trust in research results and researchers (e.g., preference on solutions from well known vendors) Lack of availability of and accessibility to relevant stakeholders Organisational culture (e.g., too bureaucratic, preference for internal knowledge production and priorities, lack of organisational knowledge sharing and collaboration, reluctance to endorse new ideas/changes/uncertainty , lack of risk management culture, secrecy attitude on security topics, short-term-focused, orthodoxy view) Language barriers (i.e., project material in English)	3 5 2 13 1
	Technological Technological infancy Further testing	1 1
	Research Limitations Lack of real data to validate research results Broad research objectives Lack of operationalisation (e.g., translate high level findings into specific actions/interventions)	2 1 6
Type	Barriers/Limitations to the uptake of research results	N. of Projects 15
Private Company	Institutional-Organisational Regulatory constrains (e.g., rigid regulations on the use of new technologies, security sensitivity, different regulations across EU) Highly politicised security markets Lack of institutional mechanisms for research transfer (from research to industry sector, from prototype to product) Lack of clear guidance and objective from stakeholders /lack of established mechanisms for translating end-users' needs into technical requirements and service specifications Organisational silos and different internal priorities Legal and organisational structure of FP7 programmes (e.g., lack of industry focus, lack of reference to EU market procurement) Lack of alignment with organisational overall priorities, or new priorities, and processes	9 3 1 3 3 2 2 4
	Financial Lack of budget to disseminate and promote research results (above all in post-research phase) Lack of post-research budget for implementation and go-to-market (e.g., to support development from prototype to product , commercialisation of research results)	5 1 4
	Cultural (including awareness-trust) Lack of understanding/awareness of research topics, results and processes (e.g., how does this result apply to me? Is it too expensive to implement? etc) Lack of availability of and accessibility to relevant stakeholders Organisational culture (e.g., preference for internal knowledge production and priorities, lack of risk management culture in some sectors, lack of collaboration with researchers, short-term-focused) Lack of trust in research results Language barriers (i.e., project material in English)	9 4 1 5 2 1
	Technological Technological infancy	1
	Research Limitations Lack of real data to validate research results Lack of focus on research as business opportunity	5 2 1

Type	Barriers/Limitations to the uptake of research results	N. of Projects
Society/Individuals	Lack of operationalisation (e.g., translate high level findings/recommendations into specific actions/interventions)	3
	Institutional-Organisational	5
	Organisational silos and different internal priorities	1
	Lack of institutional mechanisms for research transfer (e.g., implementation programmes)	1
	Lack of alignment with organisational overall priorities	2
	Lack of institutional mechanisms to involve societal actors (above all in defining research priorities)	1
	Legal and organisational structure of FP7 programmes (e.g., lack of public focus, lack of reference to EU market procurement)	2
	Lack of established mechanisms for translating end-users' needs into technical requirements and service specifications	1
	Complex and unco-ordinated stakeholder structure (e.g., too many organisations that do not coordinate activities/processes)	1
	Regulatory constrains(e.g., security sensitivity, different regulations across EU)	2
	Financial	4
	Lack of budget to disseminate and promote research results (above all in post-research phase)	4
	Cultural (including awareness-trust)	6
	Lack of understanding of research topics, results and processes (e.g., how does this result apply to me?)	1
	Lack of trust in research results (e.g., preference on solutions from well known vendors)	2
	Lack of availability of and accessibility to relevant stakeholders	1
	Organisational culture (e.g., preference for internal knowledge production and priorities, lack of inter-organisational collaboration)	3
Language barriers (i.e., project material in English)	1	
Technological		
Research Limitations	3	
Lack of operationalisation (e.g., translate high level findings into specific actions/interventions)	3	
Lack of real data to validate research results	1	

Table 3 Barriers and limitation to research uptake

Some additional general insights on the result of the investigation could be also formulated. Traditionally, security research priorities and results have mainly been defined by and directed toward governments and industry. This has meant that often the involvement of diverse and multiple security end-users in the security enterprise, above all civil organisations and individual citizens, has not been adequately represented when it comes to be on the up-taking and/or receiving end of security research outcomes. The recent shift from a state centred security concept towards a more comprehensive and citizen centred security concept, acknowledged in European¹³ and national strategies, has produced a more comprehensive approach in relation to needs, where “a growing number of programmes focus on the systemic needs of society” and address the specific needs of societal actors and organisations.”¹⁴ However, as our findings underline, when it comes to the uptake of research results by end-users, public administration and industry are still seen as the main “up-takers” of research results with society and individuals taking a back seat. All the surveyed projects, across all security dimensions, which have experienced barriers¹⁵, identify policy-makers, regulatory, administrative and enforcement agencies as their main research “up-takers” (26 projects are directed towards state actors). The majority of surveyed projects also indicate industry players as their main reference for research uptake (15 projects were also directed towards private

¹³ ESRAB, “Meeting the Challenge: The European Security Research Agenda”, September 2006

http://www.euresearch.ch/fileadmin/documents/PdfDocuments/esrab_report_en.pdf.

¹⁴ ETTIS - European Trends and Threats in Society, Seventh Framework Programme European Union, *Report on Research Approaches and Results (WP2.2)*, p. 26.

¹⁵ The researcher team of six surveyed projects indicate that no barriers were experience and the research results have been implemented as expected.

companies).¹⁶ However, only a smaller number of projects see society and individuals as active actors in the uptake of their research results (10 projects are also directed towards society).¹⁷ Indeed, the perception appears to be that society and individuals will indirectly uptake the results of research projects if public administration and industry do so. This may be due to a situation in which it has been easier to involve representatives of the private sector and public administration users in the preparatory phase of defining research priorities and subsequent research dissemination and/or uptake phase than civil society organisations.¹⁸

Another general consideration, emerging from the in-depth analysis of the surveyed projects, is related to the different experience of research uptake, which has been voiced by national and European projects. National research teams appear to be in general more positive towards the impact of the research results of their projects, irrespectively to the type of projects (i.e., new technological developments or strategic analyses) and/or security dimensions that they are addressing.¹⁹ Several researchers, involved in national programmes and/or working in national research organisations, have stressed that the overall research uptake has been successful and only a few barriers have been experienced. This is because national teams tend to have closer relationships with the main stakeholders, who are supposed to use or implement their research outcomes. Often these teams are part of and/or internal to the stakeholders' organisation. As a result they are able to engage with the end-users on a regular basis and the projects that are leading tend to have clear objectives and follow specific end-users' needs and requirements. This of course does not come as surprise but instead underlines the well-known difficulties of doing research in a pan-European environment.²⁰ Interestingly, the European projects that appear to have experienced no barriers and limitations are either the ones focusing on developing technologies for cyber security and/or support and/or pre-phase type of projects (e.g. within STReP) leading to the definition of a demonstrator project.²¹ In the former case the active involvement of the main public or industry stakeholder in the research programmes, often as member of the consortium, has allowed a closer aligned with end-users' needs and requirements and therefore fast implementation of the project results.²² In the latter, the participation of a single stakeholder, namely the European Commission, and the clear and specific objective of the project, which

¹⁶ See in the appendix: "TALOS", "INFRA", "EURACOM", "RE-DESIGN", "EFONET", "Issue Brief 4" and "SECUREAU" as example of projects whose research results are directed to industry.

¹⁷ See in the appendix: "INFRA", "BeSeCu", "EUSECON", "Global Risks", "SAFIRE", "International Crisis Group" as example of projects whose research results are directed to society.

¹⁸ See FORESEC, *Cooperation in the Context of Complexity: European Security in Light of Evolving Trends, Drivers, and Threats*, http://www.foresec.eu/wp3_docs/Foresec_report.pdf.

¹⁹ See in the appendix: "55 Trends", "Muslims in Europe", "CuteForce Analyser" and "Issue Brief No. 4".

²⁰ FORESEC, http://www.foresec.eu/wp3_docs/Foresec_report.pdf.

²¹ See in the appendix: "ACRIMAS", "CBRNEmap", "ICE", "CBRNEmap" and "ESCoRTS".

²² This probably calls for an explanation about why cyber research projects appear to attract more active and committed public and industry stakeholders. This might be due to closer alignment between cyber research programmes and end-users' priorities leading to clear and manageable objectives for the research projects. Relative easier implementation of some type of cyber technologies (e.g., cryptographic algorithms/protocols) could also play a part in facilitating research uptake in the cyber security.

is to define the focus of a new demonstrator project, have played a major part in the uptake of the research findings. Indeed, both stakeholder and project complexity is significantly reduced in this type of research projects, therefore facilitating the uptake of the research results (i.e. to agree on funding a clearly-specified demonstrator project). Furthermore, the latter projects also underline how a project-definition phase, where a few stakeholders discuss and define with the research team specific requirements and objectives for future projects, are both desirable and successful.

3.2.1 Institutional-organisational barriers and limitations

Together with cultural barriers, institutional-organisational barriers appear to be the most important in obstructing research uptake. In addition, cultural and institutional-organisational constraints are often interrelated and feed each other.

Within the institutional-organisational category, some barriers appear to dominate the uptake of research results. The most common institutional-organisational barrier and limitation is the *lack of alignment of the research project with stakeholders' overall priorities*. This is true in relation to state, industry and society (eight, four and two research projects have named this barrier for the different levels of security end-users), for all dimensions of security and type of projects (i.e., from projects dealing with technological developments to strategic analyses).²³ The lack of alignment with stakeholders' priorities can take different forms, ranging from the inability of the organisation to raise above "business as usual" activities in order to integrate research results into its operation, a strong organisational focus on immediate and short-term results, which significantly clashes with the longer time frame typical of research activities, to the existence of an organisational confirmation bias, leading potential end-users to reject research results that do not fit their priorities, artificial organisational divides between external and internal security that do not correspond to the observed reality, and sudden shifts in organisational priorities. This problem is compounded by the fact that even within the same organisation, above all within governments, priorities are not always congruent. Indeed, different and often conflicting priorities are pursued by different departments (this represents another identified barrier: *Organisational silos and different internal organisational priorities*). The above mentioned barriers point to the need for a closer co-operation of researchers with security end-users, both during the preparatory phase of defining research objectives and post-research phase of implementing research results. Both the project definition and post-research phases are identified as critical components for the uptake of research results. During the projects definition phase organisational barriers related to *lack of clear guidance and objectives from stakeholders* for strategic type of projects and/or *lack of established mechanisms for translating end-users' needs into technical requirements and service* for technology programmes are still regarded as important limitations for research uptake especially when dealing with public and industry end-users.²⁴ Furthermore, during the post-research phase *lack of institutional mechanisms for research transfer* (i.e., from research outcome to industry outcome, from prototype to product) tends to afflict technology research programmes and their uptake with industry players (three projects underline this barriers).²⁵ However, the same barrier, which often translates into lack of implementation programmes,

²³ See as example in the appendix: "EURACOM" , "SAFIRE", "RE-DESIGN" and "SECUREAU".

²⁴ See "EURACOM" and "ESRIF" for details on this organisational-institutional barrier.

²⁵ See "SECUREAU" for a discussion on this barrier.

also impacts, although with less prominence, strategic analyses directed towards state and society (one project respectively mentions this issue).²⁶

Regulatory constraints are another important limitation to the uptake of research results experienced with all security end-users and type of projects, either developing new technologies or strategic analyses. However, with the former type of projects, this relates to rigid regulations, or lack of regulations, for new technologies as well as lack of harmonisation across regulations in Europe.²⁷ In the latter this has to do with security sensitivity and classified information, which significantly hampers knowledge sharing and dissemination among all the potential research “up-takers”.²⁸ The view on secrecy as limitation appears to indicate a change in attitude in relation to national security, while calling for a constructive discussion on the necessity and appropriateness of secrecy in a security environment, characterised by a “whole-of-approach” to security involving multiple and divers actors, facing global, multifaceted and interconnected threats.

A few projects are also critical towards *the legal and organisational structure of FP7 programmes*, seen as barrier for research uptake by all the security end-users (four projects mentioned this issues in relation to state actors and two respectively in relation to industry and societal actors). This mainly relates to both the lack of flexibility of FP7 programmes, which do not allow flexible reaction to unforeseen developments in a highly innovative environment, above all for technological projects, and the lack of a clear responsibility model for the partners involved in the consortium, which makes dealing with partners’ performance very problematic. Another issue that has been stressed is the preference given to basic science research rather than policy, industry and society focused research by FP7 programmes. This constrain could be regarded as a contributing factor to another previously mentioned institutional-organisational barrier, i.e. *lack of alignment of the research project with stakeholders’ overall priorities*.²⁹

Finally more specific barriers that are related to strategic type of projects, which are directed towards public institutions and often funded and performed by national organisations, appear to be: *lack of mechanisms/feedback to monitor how strategic insights are incorporated into decision making*, and *lack of long-term political stability and therefore long-term planning*, due to government reshuffle.³⁰ The presence in Europe of *highly politicised security markets*, which require an initial political uptake of research results, is also another example of specific barriers to the uptake of research results, experienced mainly when dealing with industry players.³¹

3.2.2 Financial barriers and limitations

Financial constrains are the third most mentioned type of barriers to the uptake of research results experienced by research teams when dealing with all the security end-users (i.e., state, industry and society). In relation to government and industry this often means *lack of post-*

²⁶ See “ESRIF” for a discussion on this barrier.

²⁷ See “TALOS” and “UNCOSS”.

²⁸ See “SECUREAU” and “Muslims in Europe”.

²⁹ See “AMASS” and “FORESEC”.

³⁰ See in the appendix: “55 Trends”, “Muslims in Europe”, “Issue Brief 4” and “Strong in 21st Century”.

³¹ See “ESRIF” in the appendix.

research budget for implementation and go-to-market activities, ranging from additional funding needed to further develop prototypes into products and/or support commercialisation of research results, afflicting mainly technology type of projects, as well as lack of funding for the operational implementation of policy recommendations at national level and/or for specific contexts, concerning mainly strategic projects.³² This barrier should raise interesting questions to what extent public funding should be used to commercialise innovation, which is the route that converts ideas, research, or prototypes into viable products, services and processes, or rather market forces should be the best driver of the innovation-commercialisation path. This also calls into question *existing procurement procedures and processes*, above in relation to governments, which are viewed as to be too inflexible and rigid to support proper implementation of research results and pre-commercial innovation (one project identifies procurement processes within government as an important institutional barrier). Indubitably government and industry both play a role in establishing the environment and infrastructure necessary to support innovation and its commercialisation. Innovation and commercialisation require considerable feedback and co-operation between research and market. Deciding where public and market roles and responsibilities end and/or start often requires a complex and fine tuning. **█**

Another important financial barrier, emerging from the in-depth analysis of selected projects, is *lack of budget to disseminate and promote research results* above all in the post-research phase. This limitation appears to be critical when dealing with society but it is also important with public and industry players. Often research funding terminates when the expected research results have been achieved. This means that no funding provision is made to aggressively promote the achieved and finalised research outcome. As for some of institutional and organisation barriers, the post-research phase has again been identified as critical for the uptake of research results and therefore deserving more attention.

3.2.3 Cultural barriers and limitations

As already stressed in section 3.2.1 cultural barriers and limitations, together with institutional-organisational barriers, have emerged as the most important in obstructing research uptake. Furthermore, these two categories of constraints tend to be highly correlated and experienced simultaneously by the same project.³³

*Organisational culture*³⁴ is the typical and most mentioned constrain within this category. This applies to all security end-users (i.e., state, company and society), security dimensions and type of projects (i.e., technological and strategic programmes). Organisational culture often means: preference for internal knowledge production rather than external knowledge, developed by research teams; lack of an embedded risk management culture within the

³² See in the appendix: “INFRA”, “TALOS”, “COCAE”, “BeSeCu”, “EUSECON”, “Muslims in Europe”, “EFONET” and “SECUREAU”.

³³ See in the appendix: “AMASS”, “INFRA”, “55 Trends”, “Muslims in Europe”, “BeSeCu”, “Countering Terrorism”, “Global Risks”, “SAFIRE”, “RE-DESIGN”, “SECURENV”, “Issue Brief 4”, “FORESEC”, “Studies in Africa”, “ESRIF”, “Strong in the 21st Century”, and “Oxford Research Group”.

³⁴ Organisational culture refers here to the collective behaviour of humans who are part of an organisation and the meanings that the people attach to their actions. This includes factors such as organisation values, visions, norms, working language, systems, symbols, beliefs and habits (Hofstede, Geert, *Culture's Consequences: International Differences in Work Related Values*, Sage Publications, Beverly Hills, CA, 1984).

organisation; unwillingness to collaborate with researchers; and greater preference for short-term and quick wins. All these factors collaborate to create a pre-condition where all security end-users do not *trust research results* and prefer to implement recommendations and/or solutions by well-known commercial organisations. Furthermore, within public institutions the reluctance to endorse new ideas, change and uncertainty, which is often the by-product of research results put forward by strategic and risk type of projects, as well as a secrecy attitude on security issues and orthodoxy view of public interventions (i.e., preference for addressing symptoms rather than root-causes) are limiting the uptake of research results. This institutional reluctance appears to support a cultural mindset where only research results are taken up which are compatible with the prevailing mindsets of thinking about security in terms of threats and responses, rather than in terms of sources of security. Ironically, this type of mindset might be detrimental to societal security. Indeed, if you want to foster societal security, the defensive, secrecy-led approach of conventional security thinking is exactly the opposite of what you should do.

Lack of understanding and awareness of research topics and results has also been mentioned by some projects in relation to all the security end-users. For technological programmes this relates to a misconceived fear of high cost of commercialisation and implementation for new technologies, while for strategic type of projects this refers to the inability of end-users to understand how the research results apply to them and their specific operational contexts.

Finally, *lack of availability of and accessibility to relevant stakeholders* is the less mentioned cultural constrains. However, this still affects uptake of research results by all the security end-users.

3.2.4 Technological barriers and limitations

Technological constrains are hardly mentioned by any of the surveyed projects and only by technology programmes.³⁵The very early stage of technological innovation (i.e., technological infancy) and need for further testing tend to be associated with this category of barriers and limitations.

3.2.5 Research barriers and limitations

Similarly to financial constrains, research barriers and limitations appear to be less popular. However, they are still experienced by all the security end-users and different types of research projects, ranging from technological developments to strategic analyses.³⁶ For the former this constrain is around *lack of real data to validate new technological developments* and/or *lack of research focus on business opportunity*, which is especially relevant when dealing with the uptake of research by industry players. For the latter, research barriers are characterised by the *lack of an operationalisation and implementation component within the research output*. Indeed, such a component will allow the translation of high level findings and recommendations, which are often the output of strategic projects, into specific actions for specific end-users and their specific operational security contexts.

³⁵ Only one project, “TALOS”, has identified technological barriers as important for the uptake of research results.

³⁶ See in the appendix: “WiMA²S”, “UNCOSS”, “EUSECON”, “Global Risks”, “SECURNEV”, “Issue Brief 4”, “International Crisis Group”, “FORESEC”, “Global Trends” and “Strong in 21st Century”.

3.3 RECOMMENDATIONS FOR THE ENHANCEMENT OF THE UPTAKE OF RESEARCH RESULTS

Based on our previous findings on barriers and limitations to the uptake of research results and additional insights from the survey and interviews, conducted with the small sample of research projects, we have teased out the key cross-cutting themes for recommendation in the form of general observations and more specific insights.

Initially, some general observations regarding the requirements and practices of decision-support in the area of security are presented, which point to a silent paradigm shift in the way security issues are handled (and supported). This shift could imply the end of the special role that security research always had as compared to other research areas, and brings with it the opportunity of learning from the experiences of these other areas.

- *Observation 1: Decision- support in the area of security has become more complex and raises new requirements for both providers and users of decision support.*

As reflected in many of the projects studied, security issues are nowadays understood as highly multifaceted phenomena, which require combinations of “hard” technological, organisational and institutional enforcement mechanisms and “soft” social, economic or even cultural influences to be tackled successfully. They are seen as embedded in society and evolve as quickly as society does. As a consequence, decision-support in the field of security must cover a broad ground, use a wide spectrum and tools and methods, both at strategic and operational levels, and follow the culture and ethics of society.

- *Observation 2: It is increasingly recognised that due to the more complex security picture, more sophisticated foresight methods and risk analyses are needed as a basis for security strategy and operations. These foresight and risk assessment tools need also to become more operational and geared towards specific needs of security-end user.*

Security-related policies have to keep pace with the developments in society, economy and technology. Uncertainty is pervasive and the spectrum of future security trajectories very broad. In this light, it does not come as a surprise that sophisticated foresight approaches have become popular in the security field, as a means to structure how future security issues might look like. Complementary to foresight, similarly sophisticated risk analysis methods are needed to enable informed and seemingly rational decisions on security matters. While the projects studied point to the abundance of foresight and risk analysis approaches, the main challenge seems to reside in making them sufficiently operational to clearly guide decision-making.

- *Observation 3: The thus far dominant state-centred approach to security is increasingly challenged, while opening up opportunities for introducing novel and innovative concepts for tackling security issues into the public and policy debates.*

It is difficult to capture the ongoing changes in the perception and management of security issues in a concise way. The State-centred model has dominated our thinking for decades if not centuries, but it seems to be slowly eroding and replaced, or at least complemented, by a more decentralised model with decentralised responsibilities for ensuring security. This alternative model emphasises the need to strengthen the sources of security rather than just following a threat-response kind of thinking that has prevailed in security for long. However, the room for such novel concepts is still

limited, and they will be relevant in some areas of security only, but in line with the changing nature of security issues, they are likely to acquire greater importance in the future.

- *Observation 4: Early warning methods and tools have significantly evolved in recent years due to new developments in surveillance. Consequently, there is a need to strike the right balance, within security research programmes, among security, trust, democratic rights and the new opportunities offered by these new emerging technologies in order to build more resilient societies.*

Strengthening monitoring and surveillance capabilities has become a core research focus of several research programmes. So far this focus has been directed toward the development of new technologies with little attention to privacy and data protection. There is a need to start endorsing *privacy by design* approaches in research where privacy considerations are embedded throughout the entire life cycle of technologies, from the early design and research stage to their deployment, use and ultimate disposal.

Beyond these rather general observations on the nature of security issues and the appropriate approaches to support security policy, there are a number of more specific insights to be drawn from the analysis of barrier and opportunities to the uptake of research results in the field of security.

- *Insight 1: The early and right form of involvement of potential end- users in research and development activities needs to be given a more prominent role in security research. This is crucial for successfully making the step from testing to widespread implementation, from pilots to commercialisation.*

Research cooperation with end-users is widely recognised as important, in order to learn from their needs and requirements when developing novel solutions and insights. Often, end-users are actually quite supportive in the context of research projects. The question of uptake of research results becomes more complicated, the closer we move towards actual application of novel solutions and/or implementation of recommendations and insights. An earlier and sustainable involvement of end-users is a must. However, to ensure effective adoption of novel solutions and recommendations, a much broader approach needs to be pursued than in the past, taking the technological, organisational, institutional and cultural embedding of new solutions and recommendations very seriously. The level of engagement with end-users needs to be strongly enhanced with a combination of participatory and institutional mechanisms as well as commercially focused approaches in order to align research efforts with end-users' requirements in all relevant dimensions, while supporting post-research implementation efforts. For instance, re-enforcing the need for a pre-definition research phase in the way in which security research funding are distributed, where end-users' requirements are collected in order to define more clearly the research objectives and potential outputs, could be an example of a participatory, instructional mechanism geared to end users' engagement. Another mechanism could be funding researcher teams' short deployment and/or secondment, during critical phases of the research project cycle, to potential end-users.³⁷

³⁷ The majority of projects surveyed have indicated the need to increase end-user participation. See in the appendix: "ACRIMAS", "CBRNemap", "COCAE", "BeSeCu", "EUSECON", "Muslims in Europe", "Countering Terrorism", "Global Risks" and "SECURENV".

- *Insight 2: The State, and also industry, has a key role to play as pacemakers and lead agents in the adoption of new technological as well as non-technological approaches to tackling security issues. The ability to play that role needs to be fostered.*

There is little doubt that the state but also industry are playing a key role in shaping what threats and what solutions are regarded as important and acceptable. They are effective “lead users”, who influence what other actors might subsequently do and adopt. As a consequence, they have also a key role to play in pioneering novel solutions resulting from research and development.³⁸ The public sector, while being bound to fulfil strict requirements, has a major potential to use its procurement power more actively for piloting the introduction and use of new solutions, and thus preparing the emergence of new markets for security solutions. Furthermore, it could also support more aggressively commercialisation and implementation efforts by providing both funding and innovative mechanisms to allow successful research-market transfer. In other words, the state can play a pivotal role in reducing barriers to adoption.³⁹

- *Insight 3: The cultural (and sometimes institutional-organisational) barriers to adoption need to be taken much more seriously. Conservatism and risk-averseness are well established virtues in the security field, but they hinder the introduction of new promising solutions and insights.*

From the perspective of an individual organisation, there are always many good reasons for non-adopting new solutions to security issues and for not opening up to other organisations: lack of trust in solutions developed elsewhere (“not-invented-here”), fear of significant disruption to business-as-usual, preference for short-term and quick wins, unwillingness to endorse risk and uncertainty are only a few of the most mentioned cultural and institutional organisational barriers. Dealing with these issues requires a systemic rather than a piecemeal approach geared towards rewarding innovation successes and its promoters. This systemic approach should address all underlying and interrelated root causes of innovative adoption, namely: leadership and organisation; processes and tools; people and skills; and culture and values.⁴⁰ Strategies to address root causes of innovation should then be in place together with research programmes to create a more responsive environment to innovative adoption.

- *Insight 4: The diversity and rigidity of security-related regulations in Europe are too high. They prevent new security technologies and options to be adopted quickly.*

Security organisations have a long-standing tradition of relying on secrecy to protect their knowledge. In times of European integration and demand for enhanced collaboration to tackle security issues among a much broader and diverse number of active stakeholders, ranging from private companies to civil organisations and individuals, this is counter-productive. EU institutions and Member States will have to treat security as a co-operative arena that does not lend itself to rigid institutional

³⁸ Similar recommendation has been voiced by ESRIF. See ESRIF, *Final Report*, 2009, http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

³⁹ Some of the projects surveyed put forward as recommendations the development of post-research funding mechanisms that could be support commercialisation and implementation of research findings. See in the appendix: “TALOS”, “EURACOM”, “BeSeCu”, “Global Risks”, “SAFIRE”, “RE-DESIGN”, “EFONET”, “SECUREAU” and “ESRIF”.

⁴⁰ Fagerberg, Jan, David C. Mowery and Richard R. Nelson, *The Oxford Handbook of Innovation*, Oxford University Press, Oxford, 2006.

divisions but instead places a premium on integration and coordination of knowledge, experience and responsibilities. The place for secrecy as pillar of national security will need to be reevaluated in light of all these changes. Furthermore, the existence of different regulations across Europe in relation to security and new technologies stand in the way of commercially viable implementations and exploitations of research results. Specifically, the EU could adopt common policy and regulations on the adoption of new surveillance and monitor technologies, the use of new weapons and the use of newly security related technologies on private facilities but also on how to deal with the ethical, legal and social impact of security technologies and policies. Indeed renewed efforts on the regulatory front, led by the European Union, is still required.⁴¹

- *Insight 5: There is a conceptual issue that contributes to slowing down the uptake of new security solutions, which consists of the perseverance of established mental frameworks and way of thinking about security issues. Opening up mindsets is thus a major issue for accelerating the uptake of research results, and it should be given a more prominent role in security research.*

As long as security issues are conceived of as matter of responding with appropriate capabilities and assets to emerging threats, many innovative security solutions and recommendations are unlikely to be adopted. The reason is that their effectiveness is only credible in the context of a different way of conceiving of security issues. If, for instance, security is understood more in the sense of strengthening the sources of security in society rather than just responding to threats, new and different security options come into play and could potentially be adopted.⁴² Part of the responsibility of driving this mindset change could be given to research programmes as a component of their stakeholder communication and engagement strategy.

- *Insight 6: EU-funded security research projects are confronted with a number of specific barriers to uptake. Both the practice and the regulations of EU security programmes need to be adjusted in order to make the outcomes more attractive to potential users of research results.*

There are several reasons for the relative ineffectiveness of EU-funded research. The rigidity and inflexibility of EU-research frameworks' regulations make the adaptation of work plans difficult, and thus the adaptation to emerging insights about user needs and new developments in the course of a project. EU research is often simply too far

⁴¹ The need for regulatory harmonisation has already been underlined by ESRIF. ESRIF's recommendations includes: the development of a common, harmonised regulatory framework for security technologies and security research and innovation in Europe, and a more harmonised European procurement process and security market achieved via common standards, validation and certification processes as well as common rules and procedures. See ESRIF, *Final Report*, 2009. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

⁴² Emphasis on changing mindset has been underlined by "55 Trends", "Global Risks", "RE-DESIGN", "SECURENV", "Issue Brief No. 4, "International Crisis Group", "Oxford Research Group" and "FORESEC". In particular FORESEC report argues that shifts in mindset can be supported by the re-formulation of science and technology priorities as well as the re-allocation of research and development funds (FORESEC, *Cooperation in the Context of Complexity: European Security in Light of Evolving Trends, Drivers, and Threats*, 2009. http://www.foresec.eu/wp3_docs/Foresec_report.pdf).

away and too time-consuming (i.e., three years are a very long time in a commercial environment) from the reality of security practitioners and end-users to be seriously considered.⁴³ Moreover, managing European consortia in order to achieve research results that could be up-taken by end-users is often difficult given the lack of performance monitoring and enforcement mechanisms for the consortium partners. Finally, the availability of the knowledge generated by EU project to potential users is hampered by the absence of appropriate mechanisms to store and upgrade that knowledge in the light of practical learning experiences. There is a need to continually communicate research results, even after the end of the research programmes, monitor application and impact of the knowledge produced, and maintain an institutional knowledge base on the research work and its outcomes.

4 ANNEX 1: SECURITY TAXONOMY

	Intergovernmental organisations	States	Companies	Civil society	Individuals & households
Physical security Definition: Dimension of security concerned with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings	<ul style="list-style-type: none"> Protection of the international state system Protection of transnational infrastructures and physical assets (e.g., transnational pipelines, etc.) Protection of the physical existence of global citizens 	<ul style="list-style-type: none"> Protection of national territory (e.g., borders, sea, etc.) Protection of national spaces and buildings (e.g., cities, squares, monuments) Protection of national infrastructures and physical assets (e.g., transport, electricity system) Protection of the physical existence of citizens 	<ul style="list-style-type: none"> Protection of corporate buildings (e.g., offices, depots, etc.) Protection of corporate infrastructures and physical assets (e.g., IT and communication infrastructures) Protection of employees' lives Protection of consumers' lives 	<ul style="list-style-type: none"> Protection of society's physical assets (e.g., spaces and buildings) Protection of society's infrastructures (e.g., communication infrastructures, educational infrastructures) Protection of civilians' lives 	<ul style="list-style-type: none"> Protection of one's own body and health Protection of one's own properties and physical assets (e.g., house, car)
Political security Definition: Dimension of security concerned with the protection of acquired rights, established institutions and recognised policy choices. Political security measures the absence of threats to these rights, institutions and choices as well as the absence of fear that such rights and institutions and choice could be attacked.	<ul style="list-style-type: none"> Protection and development of international regimes, institutions and norms Protection of universally recognised rights for humanity (e.g., declarations of human rights) 	<ul style="list-style-type: none"> Protection of established international norms and institutions within the international context Protection of national law, norms and institutions Protection of citizens' freedom and nationally acquired rights 	<ul style="list-style-type: none"> Protection of employees' rights (e.g., contract of employment, racial discrimination, age discrimination, training rights) Protection of consumers' rights (e.g., purchase rights, quality rights) Protection of shareholders' rights (e.g., to pass resolutions, to call special meetings) 	<ul style="list-style-type: none"> Protection of society's established institutions and organisational principles (e.g., family structure, social solidarity, representation rights through trade unions) 	<ul style="list-style-type: none"> Protection of one's own freedom and rights Freedom from fear and oppression

⁴³ A recent assessment of FP7Sec projects also underlines that although “many projects have been successful in engaging with users, others have experienced difficulties in securing end-user engagement.” This is due to several obstacles ranging from limited human resources and the busy schedule of users, and a lack of interest in engaging directly in security research projects unless research was ‘near to market’(Centre for Strategy and Evaluation Services , *Ex-post Evaluation of PASR and Interim Evaluation of FP7 Security Research. Executive Summary*, 2011. http://ec.europa.eu/enterprise/dg/files/evaluation/01_executive_summary_security_en.pdf)

	Intergovernmental organisations	States	Companies	Civil society	Individuals & households
<p>Socio-economic security</p> <p>Definition: Dimension of security concerned with socio-economic measures designed to safeguard the economic and social system, its development and its impact on individuals</p>	<ul style="list-style-type: none"> Protection and growth of a sustainable international socio-economic context, both in relation to its functioning and structure. This includes maintenance of a fair, safe, secure and dynamic international environment Ability to encourage and sustain long term international socio-economic improvements Protection of socio-economic well-being of global humanity 	<ul style="list-style-type: none"> Protection and growth of a sustainable national socio-economic context, both in relation to its functioning and structure. This includes the maintenance of a fair, safe, secure and dynamic national socio-economic environment Ability to encourage and sustain long-term national socio-economic improvements Maintenance of a fair, safe, secure and dynamic national socio-economic environment Protection of socio-economic well-being of citizens Freedom to follow choice of policies to develop a nation's socio-economic environment in the manner desired by the state 	<ul style="list-style-type: none"> Protection of corporate economic assets, both tangible and intangible (e.g., market shares, brand value) Ability to encourage and sustain long term corporate growth Protection of employees' economic and social well-being 	<ul style="list-style-type: none"> Protection of society's socio-economic assets, both tangible and intangible Ability to encourage and sustain long-term societal welfare Protection of civilians' socio-economic well-being 	<ul style="list-style-type: none"> Protection of one's own current and future employment, sources of income and social relationships Protection of one's current and future social well-being Freedom from want
<p>Cultural security</p> <p>Definition: Dimension of security concerned with measures designed to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices while allowing for changes that are judged to be acceptable</p>	<ul style="list-style-type: none"> Protection of diverse and pluralistic cultures Promoting the international growth of diverse international cultures in their own accord 	<ul style="list-style-type: none"> Protection of national cultures Promoting the growth of national cultures by maintaining cultural differences Protection of citizen's diverse cultural identity 	<ul style="list-style-type: none"> Protection of corporate culture (e.g., corporate values, missions statement) Promoting growth of corporate culture Protection of employees' cultures 	<ul style="list-style-type: none"> Protection of a set of distinctive spiritual, material, intellectual and emotional features of society and diverse social groups. This encompasses, in addition to arts and literature, lifestyle, ways of living together with value systems, traditions and beliefs Promoting the growth of society and diverse social groups' culture 	<ul style="list-style-type: none"> Protection of one's own set of beliefs, traditions and values. This encompasses one's own personal lifestyle and way of living
<p>Environmental security</p> <p>Definition: Dimension of security concerned with measures designed to provide safety from environmental dangers including diseases caused by natural or human processes due to ignorance, accident, mismanagement or intentional design, and originating within or across national borders</p>	<ul style="list-style-type: none"> Protection of international environment and natural resources across national borders and social divisions Promoting sustainable development internationally Prevention and response to environmentally caused transnational threats/risks (e.g., climate change, environmental degradation, food and resource scarcity, diseases) Provide global humanity with safe access to and strategic use of environment and 	<ul style="list-style-type: none"> Protection of national environment and natural resources across social divisions Promoting sustainable development nationally Prevention and response to environmentally caused national and transnational threats/risks (e.g., climate change, environmental degradation, food and resource scarcity, diseases) Safe access to and strategic use of environment and natural resources for citizens 	<ul style="list-style-type: none"> Compliance with environmental law, meeting international standards, as well as best practices Safe and sustainable access/use of natural resources needed for production Promoting sustainable development in operating markets 	<ul style="list-style-type: none"> Protection of society's environment and natural resources across social divisions Promoting sustainable development within society Prevention and response to society's environmentally caused threats and risks (e.g., water and air degradation) Safe access and strategic use of environment and natural resources for civilians 	<ul style="list-style-type: none"> Protection of one's own individual ecosystem Protection of one's own individual access and safe use of natural resources Individual prevention and response to environmentally caused threats and risks (e.g., flood, pollution, diseases)

	Intergovernmental organisations	States	Companies	Civil society	Individuals & households
	natural resources				
Radical uncertainty security Definition: Dimension of security concerned with measures designed to provide safety from exceptional and rare violence and threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life	<ul style="list-style-type: none"> Protection of global humanity from radical uncertainties (e.g., natural hazards, pandemics) Increasing the resilience of the international community 	<ul style="list-style-type: none"> Protection of citizens from radical uncertainties (e.g., natural hazards, pandemics) Promoting and increasing national resilience 	<ul style="list-style-type: none"> Protection of employees from radical uncertainties (e.g., natural hazards, pandemics) Promoting and increasing corporate resilience 	<ul style="list-style-type: none"> Protection of civilians from radical uncertainties (e.g., natural hazards, pandemics) Promoting and increasing societal resilience 	<ul style="list-style-type: none"> Preparing for sudden emergencies Developing individual resilience
Cyber security Definition: Dimension of security concerned with measures designed to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction	<ul style="list-style-type: none"> Protection of information and information systems across national borders and state divisions Promoting safe access, use and development of information across national borders Protecting identity and information produced by a global and diverse humanity 	<ul style="list-style-type: none"> Protection of national information and information systems Promoting safe access, use and development of national information Protection of identity and information produced by citizens 	<ul style="list-style-type: none"> Protection of corporate information and information systems Assure compliance with information law, meeting international standards, as well as best practices Promoting safe access, use and development of corporate information Protection of identity and information produced by employees and consumers 	<ul style="list-style-type: none"> Protection of society's information and information systems Promoting safe access, use and development of social information Protection of identity and information produced by social groups and civilians 	<ul style="list-style-type: none"> Protection of one's own information, information system, identity and privacy Safe access, use and development of one's own information and identity

Table 4 Dimensions of Societal Security⁴⁴

⁴⁴ See ETTIS - European Trends and Threats in Society, Seventh Framework Programme European Union, *Report on Research Approaches and Results (WP2.2)*, pp. 12-14.