European Foresight Platform
supporting forward looking decision making
www.foresight-platform.eu

EFP Deliverable 2.4 – WP 2 – SUPP – Public

2nd EFP Annual Mapping Report: *Security Futures*

Towards a Fully-Fledged Futures Mapping: Results of Mapping 16 FLAs on Security

Date: December 2012

Authors: Effie Amanatidou (The University of Manchester)
Rafael Popper (The University of Manchester)
Thomas Teichler (Technopolis Group)

With contributions from:

- Elisabetta Marinelli (JRC),
- Annelieke van der Giessen and Bas van Schoonhoven (TNO)
- Ivan Montenegro Trujillo (Colciencias)
- Guillermo Velasco (PhD researcher at The University of Manchester)
- Monika Popper (MSc student at The University of Manchester)

European Foresight Platform

The European Commission is providing the means to continue the important networking activities of foresight initiatives. Setting out on the previous work of the European Foresight Monitoring Network and For-Learn the new European Foresight Platform resumes its work.

Project funded under the Socio-economic Sciences and Humanities

About the 2nd EFP Annual Mapping Report: Security Futures

This report represents deliverable 2.4, of the EFP project. The report discusses the key findings and lessons from the examination of 16 FLAs mapped in the area of security research. After exploring the features of the mapped cases across the different mapping variables the report tries to identify similarities and differences and to provide an overall picture of the type of research and outcomes carried out in the area of security.

Date: December 2012

Authors:

Effie Amanatidou	MIoIR/University of Manchester	Effie.amanatidou@gmail.com
Rafael Popper	MIoIR/University of Manchester	Rafael.popper@mbs.ac.uk
Thomas Teichler	Technopolis Group	Thomas.teichler@technopolis-group.com

About the European Foresight Platform (EFP)

The EC under its Seventh Framework Programme for Research and Technology Development (FP7) is providing the means to continue the important networking activities of foresight initiatives. The Coordination and Support Action "EFP European Foresight Platform – supporting forward looking decision making" aims at consolidating the information and knowledge base on foresight in Europe and internationally. The ultimate purpose of EFP is to better exploit foresight as a resource to support policy-making. The knowledge hub will be used in a series of national and European policy workshops, geared towards major future challenges to Europe. For more information about EFP please visit http://www.foresight-platform.eu and to explore more cases in detail please visit http://www.mappingforesight.eu

About the EFP Consortium

The EFP Consortium consists of the Austrian Institute of Technology (AIT), the largest non-university research organization in Austria, which is active in front-end research with national, European and global reach. The Institute for Prospective Technological Studies (IPTS) is one of the seven scientific institutes of the European Commission's Joint Research Centre and located in Seville, Spain. The Netherlands Organisation for Applied Scientific Research (TNO) is a leading public research organisation in the Netherlands. Its department of Strategies for the Information Society counts 25 researchers and is specialised in policy research related to ICT, media and innovation. The Manchester Institute of Innovation Research (MIoIR) is the research centre of excellence in the Manchester Business School (MBS) and The University of Manchester in the field of innovation and science studies. With more than 50 full members and a range of associated academics from across the University, MIoIR is Europe's largest and one of the World's leading research centres in this field.

EUROPEAN COMMISSION
European Research Area

SEVENTH FRAMEWORK PROGRAMME

Funded under Socio-economic Sciences & Humanities

European Foresight Platform

The European Commission is providing the means to continue the important networking activities of foresight initiatives. Setting out on the previous work of the European Foresight Monitoring Network and For-Learn the new European Foresight Platform resumes its work.

Acknowledgements

We wish to thank those experts and colleagues who have supported us in the preparation of this report. In particular our thanks are due to our colleagues from AIT, IPTS and TNO for their invaluable comments on drafts of this report, in particular to Ivan Montenegro Trujillo (Colciencias and 2012 Academic Visitor at Manchester Institute of Innovation Research), Annelieke van der Giessen, Bas van Schoonhoven, Dirk Johann, Elisabetta Marinelli, Joachim Klerx, Matthias Weber and Susanne Giesecke, as well as to the design elements and the royalty-free license our IT subcontractor (Cyber Fox) received from Futures Diamond in order to use its Background Intellectual Property (mapping and content management system) for the purpose of delivering an independent Mapping Environment supporting the EFP Mapping Work Package (WP2). Finally, we wish to thank Guillermo Velasco and Monika Popper for contributing to the European Commission efforts to map forward-looking activities (FLAs) around the world.

Foreword

This 2nd European Foresight Platform Annual Mapping Report (**2nd EFP-AMR**) represents a major step forward in the successful implementation of the *SMART Futures* approach: A fully-fledged futures mapping framework described and piloted in the 1st EFP-AMR.

On the one hand, the report puts in evidence that the breadth and depth of the EFP mapping activities are substantially bigger in scope than our previous mapping efforts in the European Foresight Monitoring Network (EFMN). Three specific mapping strategies demonstrate this: first, the mapping of a wider range of forward-looking activities (FLAs), such as foresight, horizon scanning and technology assessment, for example; second, the use of 33 elements in 3 complementary types of mapping including *practices*, *players* and *outcomes*; and third, the use of 16 case studies to cover FLAs on ***Security***. On the other hand, the report highlights the future potential of larger scale and targeted mapping of FLA *outcomes*. Of course, it is important to continue mapping *practices* – to improve the way we conduct and evaluate FLAs; and *players* – to identify key stakeholders, institutions and individuals with whom to establish possible collaborations but also to have a map of players actively shaping our images of the future.

The 2nd EFP-AMR on ***Security Futures*** should be read bearing in mind that it is part of a "bigger picture". Since 2004 the foresight team of the University Manchester has been improving the methodology to map forward-looking activities. The "SMART Futures Jigsaw" has proven a promising framework to study more than thirty elements characterising FLA. A substantial amount of data has been generated in the 16 cases mapped and many more cases (potentially hundreds) should be mapped in the years to come. However, due to limited resources in EFP, the project consortium and the EC agreed to set modest but well-planned incremental targets, so the next report is expected to cover *20 cases on Health*. Furthermore, having our long-term FLA mapping objectives in mind (i.e. post-EFP mapping), we have developed a bottom-up strategy that allows the FLA community to map additional cases using a web-based crowdsourcing approach. This is why the mapping work uses a fully independent system (available online at www.mappingforesight.eu), which has been carefully aligned to the needs of the EFP Mapping Environment, and that of other FLAs at international and national levels.

Another important consideration of the "bigger picture" of our mapping work is that it is inherently linked to the strategic information needs of a wide range of stakeholders including government, business, research and education actors at local, national and international levels. With this in mind we started to develop some guidance for difference audiences reading our future reports. For this reason, we have included a section on "How to read the 2nd EFP Annual Mapping Report" in order to give some indications about mapping results that may be particularly relevant for: decision-makers and policy-shapers; thematic experts; civil society, NGOs; business people; and FLA practitioners.

Obviously, as our Mapping work will continue evolving beyond the life of the EFP project, we will appreciate your feedback on the 2nd EFP-AMR and encourage you to register and proactively contribute to our mapping work.

Dr Rafael Popper
Manchester Institute of Innovation Research

Table of Contents

List of Tables

List of Figures

List of Boxes

1 Introduction

EFP mapping aims at creating a valuable repository of knowledge on forward-looking activities (FLAs) to serve as source material informing and supporting national and pan-European policy processes. EFP will use tools to examine the contours of FLAs, and how they are changing, in evidence-based ways, from a variety of perspectives (Popper and Teichler, 2011).

The present report represents the 2nd EFP Annual Mapping Report (**2nd EFP-AMR**)[1]. The report aims to discuss key findings and lessons from the mapped FLAs in the area of security and to construct an overall picture of the type of forward-looking research carried out in the area.[2]

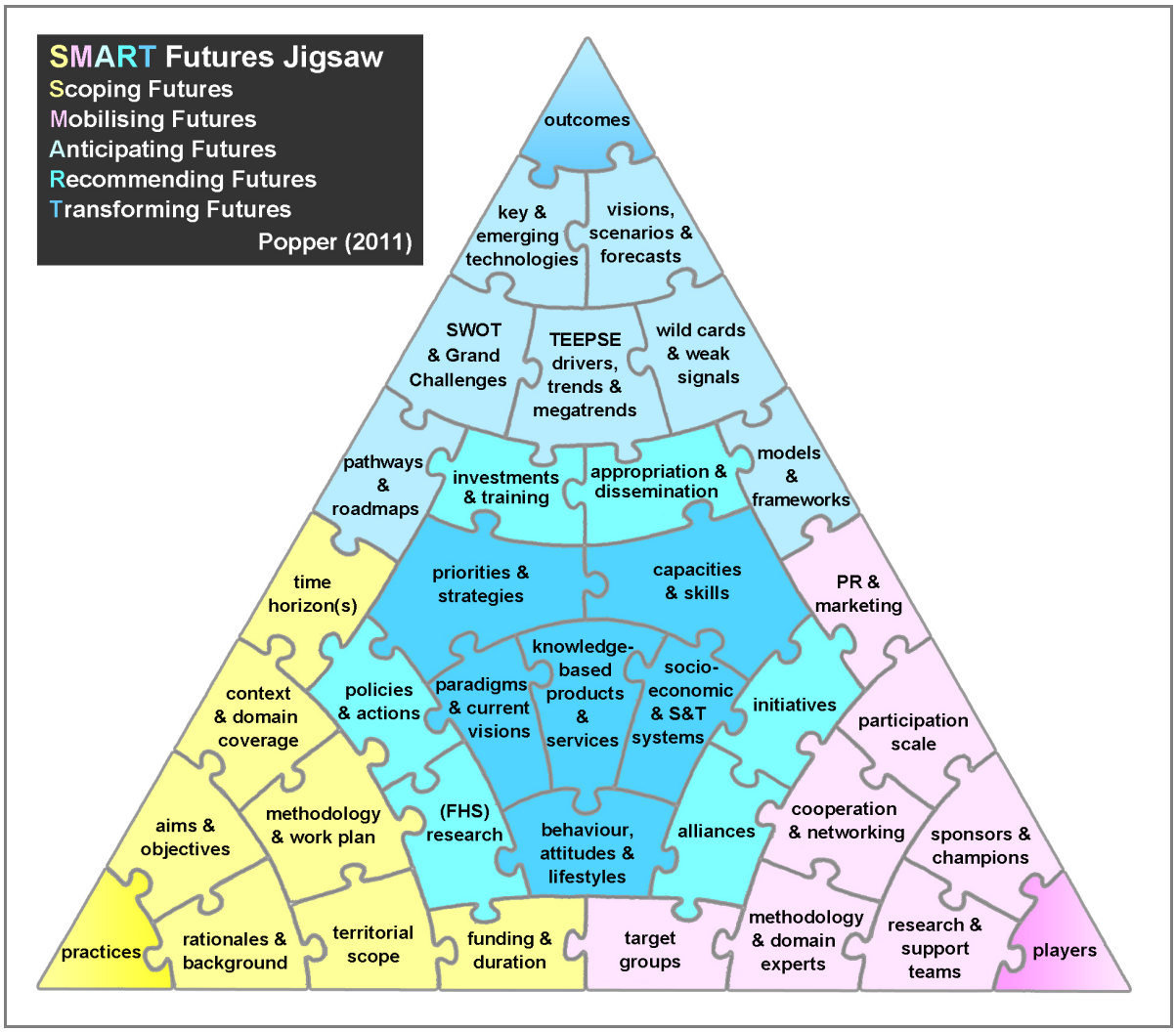
Overall, the mapping methodology involved both primary and secondary research approaches. The former type included interviews with sponsors, practitioners and users of the cases mapped; the latter referred to documentary analysis of academic and grey literature about the selected FLAs. The elaboration of the findings from the mapped FLAs was based on statistics (that were enabled by the mapping environment) and also on the 'intelligent reading' by the authors of the report who are experts in foresight and the domains covered.

The conceptual basis for mapping foresight and forward-looking activities is represented in the SMART Futures Jigsaw (Popper, 2011). It contains 36 elements, which are the dimensions along which we will map FLA. They related to the different phases of a FLA: *scoping*, *mobilising*, *anticipating*, *recommending* and *transforming*. Each of these phases and elements will be explained in greater detail below.

1 The 3rd EFP-AMR is focused on health-related FLAs.

2 Although 3 out of the 15 cases are not EU projects, most of the security FLAs are projects funded by the EC Framework Programmes. Thus, in realistic terms the overall picture will describe the type of FLA research in the area of security supported by the EU.

Figure 1: The SMART Futures Jigsaw



Source: Popper, 2011

The "scoping futures" phase corresponds to the FLA practices, the "mobilising futures" corresponds to the FLA players, and the "anticipating", "recommending", and "transforming futures" phases are represented by the FLA outcomes. The structure of the report follows the structure of the EFP mapping environment, i.e. practices (Section 2.1), players (Section 2.2) and outcomes (Section 2.3).

More specifically, the results cover the following indicators under each mapping dimension:

- Practices: aims and objectives, rationales, context and domain coverage, methodology, territorial scope and time horizon;
- Players: sponsors, target groups, public relations (PR) and marketing;
- Outcomes: anticipating futures, recommending futures and transforming futures

1.1 How to read the 2nd EFP Annual Mapping Report?

The EFP mapping enables the mapping of FLAs across three major dimensions characterising FLAs (practices, players and outcomes) each one comprising several indicators. While not all the indicators are addressed in the present report (mainly due to lack of available information or non-relevance of the indicator to the specific case) the analysis presented herewith may prove useful for different audiences in different ways.

In particular, decision-makers and policy-shapers as well as the so-called end-users represented by society organisations, NGOs, etc. may find particularly useful the presentation of outcomes. It would be interesting to see the challenges identified and the resulting scenarios and visions for the EU or NATO. At the same time, the "trends and drivers" analysis is useful especially when these focus on identified grand challenges followed by possible technological solutions or policy recommendations. The research strategies and/or priorities identified are of equal importance. As a result, sections 2.3 (FLA outcomes) will be particularly interesting for this type of audiences.

Thematic experts may be attracted by the "mobilising futures" phase in meeting their efforts to identify other experts around the world to expand their networks and possibly move to collaboration activities. They will probably be interested in identified critical and key technologies that seem promising in providing solutions to current challenges, as well as by wild cards and weak signals with strong potential to change certain scientific and technological fields. The numerous models and frameworks resulting from methodologically oriented FLAs may also be of interest to theme experts as well as FLA practitioners.

FLA practitioners may be interested in all the different phases but maybe more in the "scoping" and "mobilising futures" phases as these are more oriented towards the methodological and implementation elements of FLAs. Business people may find particularly useful the analysis of key trends and drivers both in a generic mode covering 'horizontal' (rather than theme-specific) evolutions as well as in a theme-specific mode addressing the field of security. Scenarios and possible technological solutions are also of particular interest to businesses as inputs to their strategy development.

Table 1: Mapped cases for the 2nd Annual Mapping Report

Target audience	Indicative sections of high relevance
Decision-makers and policy-shapers	2.3
Thematic experts	2.2; 2.3.1
Civil society, NGOs	2.3
Business people	2.3.1
FLA practitioners	2.1, 2.2, 2.3.1

2 Mapping of FLA cases

In total the mapped cases where the present report is based on are the following.

Table 2: Mapped cases in the area of security for the 2nd Annual Mapping Report

Project Title	Acronym	Specific Progr./Theme	Coord. Country	Type of FLA
1. DCDC Global Strategic Trends 2040		SECURITY	UK	Forecasting
2. ESPAS Global Trends 2030		SECURITY	EU	Forecasting
3. NIC Global Trends 2025		SECURITY	US	Forecasting
4. Europe's evolving security: drivers, trends and scenarios	FORESEC	SECURITY	FI	Foresight
5. The future impact of security and defence policies on the European research area	SANDERA	SECURITY	UK	Foresight
6. Changing Multilateralism	EU-GRASP	SECURITY	BE	Foresight
7. Foresight of evolving security threats posed by emerging technologies	FESTOS	SECURITY	IL	Horizon Scanning
8. Security Jam 2012		SECURITY	NATO	Horizon scanning
9. Privacy awareness through security branding	PATS	SECURITY	DE	Impact assessment
10. Strategic Risk Assessment and Contingency Planning in Interconnected Transport Networks	STARTRANS	SECURITY	LU	Impact Assessment
11. Aftermath Crisis Management System-of-systems Demonstration	ACRIMAS	SECURITY	DE	Impact Assessment
12. Security of road transport networks	SERON	SECURITY	DE	Impact Assessment
13. EUropean Risk Assessment and Contingency planning Methodologies for interconnected networks	EURACOM	SECURITY	BE	Impact Assessment
14. Assessment of Environmental Accidents from a Security Perspective	SECURENV	SECURITY	HU	Impact Assessment
15. Decision support on security investment	DESSI	SECURITY	DK	Impact Assessment
16. Security Technology Active Watch	STRAW	SECURITY	ES	Impact Assessment

According to the 1st EFP Annual Mapping Report (Popper and Teichler, 2011), the European Foresight Platform (EFP) broadened the scope of its mapping activities in comparison with past activities like EFMN in order to study main practices, players and outcomes of selected *foresight*, *forecasting*, *horizon scanning* and *impact assessment* (e.g. technology or risk assessment) studies.

The 16 FLAs represent all three types. However, some points are worth noting here. Historically security FLAs have been carried out by military strategists, e.g. in Ministries of Defence, at

universities and dedicated think tanks. While these have combined experts from a variety of fields including history, economics, and politics, the emphasis on statistical modelling of the 1950, 60s and 70s has given way to a more qualitative engagement with strategic issues that is more akin to foresight work. This is not to say that technology assessments or econometric analyses are not done in this area. However, they are more supportive rather than guiding the work nowadays.

Secondly, the main developments in security policy and academic security research in the past two decades are mainly linked to conceptual and institutional rather than technological innovations. Since the end-1980s the concept of security has been altered to mean more than 'merely' a state of safety for the nation state mainly achieved by military means. No doubt, technological developments are among the factors that have led to such changes – as are the end of the cold war, the foundation of the European Union, continued and accelerating globalisation and Europeanisation. However, the emphasis has been on new concepts, policies and institutions, phenomena that appear to be more adequately captured by foresight than by forecasting methods.

Thirdly, and here a certain selection bias plays out, most cases under consideration are FP7 funded studies. In other words, the mapping has so far focused on EU security studies and, therefore, on projects dealing with security at EU level. Traditionally, security and defence issues have not loomed large among EU policies, as this topic has been a (tightly guarded) domain of member states' governments and subject to bi- or multilateral cooperation among them. Consequently, the EU security policy field is still being formulated. This is another reason why foresight–related methodologies (emphasising conceptual aspects, vision building and close engagement of all relevant stakeholders).

A last point to make is that 'impact assessment' as well as 'forecasting' studies usually take the form of 'risk assessments' in the field of security. These mainly deal with identification of trends (as in the two forecasting cases in the table) or estimation and managements of threats and risks of various types (environmental accidents, risks in transportation and inter-connected networks, crises management, etc.).

Geographically speaking, the mapped cases mainly refer to the EU region. However, they may also cover non-EU countries like the US (PATS, NIC Global Trends 2025) or have no specific geographical scope such as the NATO study (Security Jam, 2012).

2.1 Scoping futures - Results on FLA practices

Drawing upon the SMART jigsaw, FLA practices represent the scoping phase of FLAs. As noted above the indicators covered in the present report under the FLA practices are aims and objectives; rationales; domain coverage, territorial scope and relevance for EU.

2.1.1 Aims and objectives

The security theme of EC FP7 gives emphasis in increasing security of citizens, infrastructures and utilities; intelligent surveillance and border security; restoring security and safety in case of crisis; improving security systems integration, interconnectivity and interoperability; studying socio-economic, political and cultural aspects of security, ethics and values; and supporting security research coordination and structuring. In this regard, in the security FLAs 'security' is

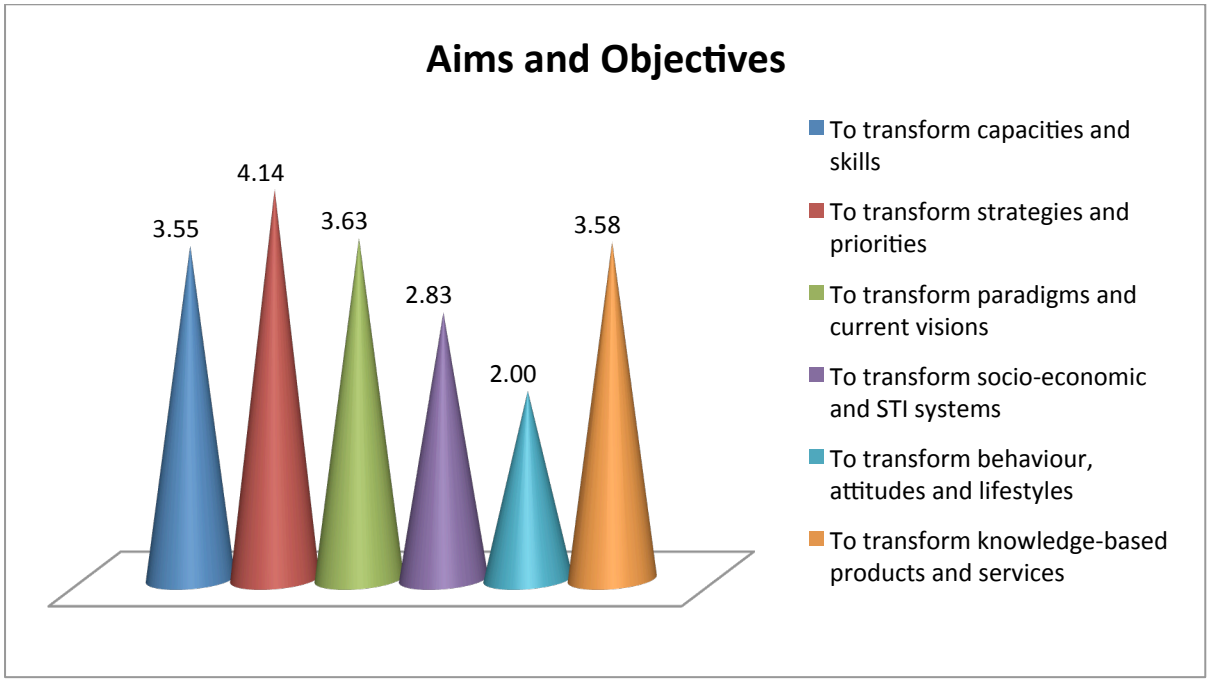
understood in a broad sense: a referent object (state, society, human being) is to be 'care free' (from hazards, threats etc.) and might take action to this end (prevent, protect, defend, insure or increase resilience).[3]

As a consequence the FLA studies under consideration:

- examine future developments in defence and homeland security;
- look at internal and external dimensions of security;
- address the security of various referent objects;
- examine the evolvement of different types of threats; and
- discuss policy or conceptual developments.

Within this framework, the main aims of the FLAs in the security area have been 'to transform strategies and priorities' and also 'current visions and paradigms', as well as 'capacities and skills'. The next major aim is to 'transform knowledge-based products and services'. Overall, there is a focus on an ambition towards common activities and shared ways of doing things, which may reflect the fact that European security policy has not yet reached a degree of maturity. At the same time there is a trend to improve capacities, skills and services provided. This is reflected mainly in FLAs that aim also at producing certain models for risk assessment and management or analytical and conceptual frameworks.

Figure 2: Aims of security – related FLAs



EFP mappers had the opportunity to choose from 1 to 5 stars to show relevance of aims to the specific FLA. The number shown on top of each bar is the mean of these scores.

2.1.2 Rationales

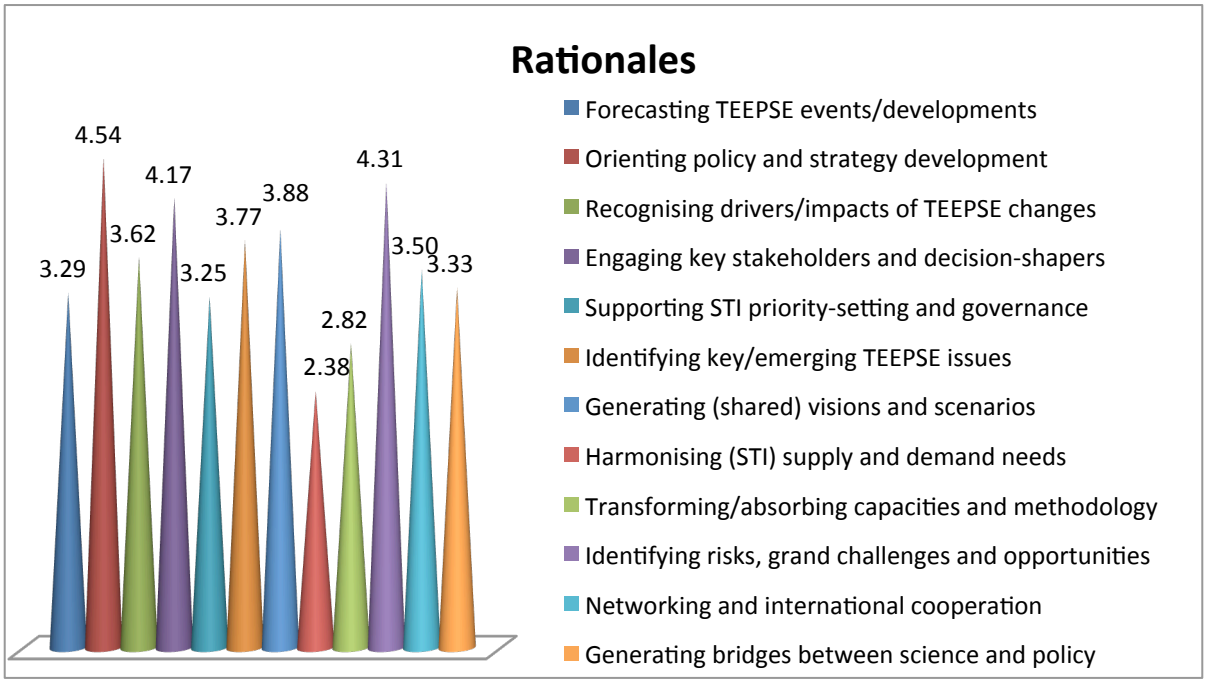
Apart from 'orienting policy and strategy development' the main rationale for conducting FLA in the security area has been to 'engage key stakeholders and decision shapers'. This is not

[3] http://cordis.europa.eu/fp7/security/home_en.html last accessed 27 February 2012.

surprising given the focus on EU level security issues of the FLA activities under consideration here. European Security and Defence Policy is still in its formative period; the relevant stakeholders used to a national framework of reference are yet to be linked; institutions and mind frames geared towards transatlantic cooperation need to be altered to include a layer of European collaboration. Closely related to this most important rationale of FLAs in the security domain is the notion 'to generate shared visions and scenarios' of European security. The latter can be regarded as a means to engage stakeholders and decision shapers in a meaningful way and to initiate a process in which they start addressing the issue area of security in a new way.

At the same time, 'identifying risks, grand challenges and opportunities' is among the most important rationales. This type of rationale mainly reflects the focus of the risk assessment studies mapped along with 'identifying key/emerging TEEPSE issues' and 'recognising drivers/impacts of TEEPSE changes'.

Figure 3: Rationales of security FLAs



EFP mappers had the opportunity to choose from 1 to 5 stars to show relevance of aims to the specific FLA. The number shown on top of each bar is the mean of these scores.

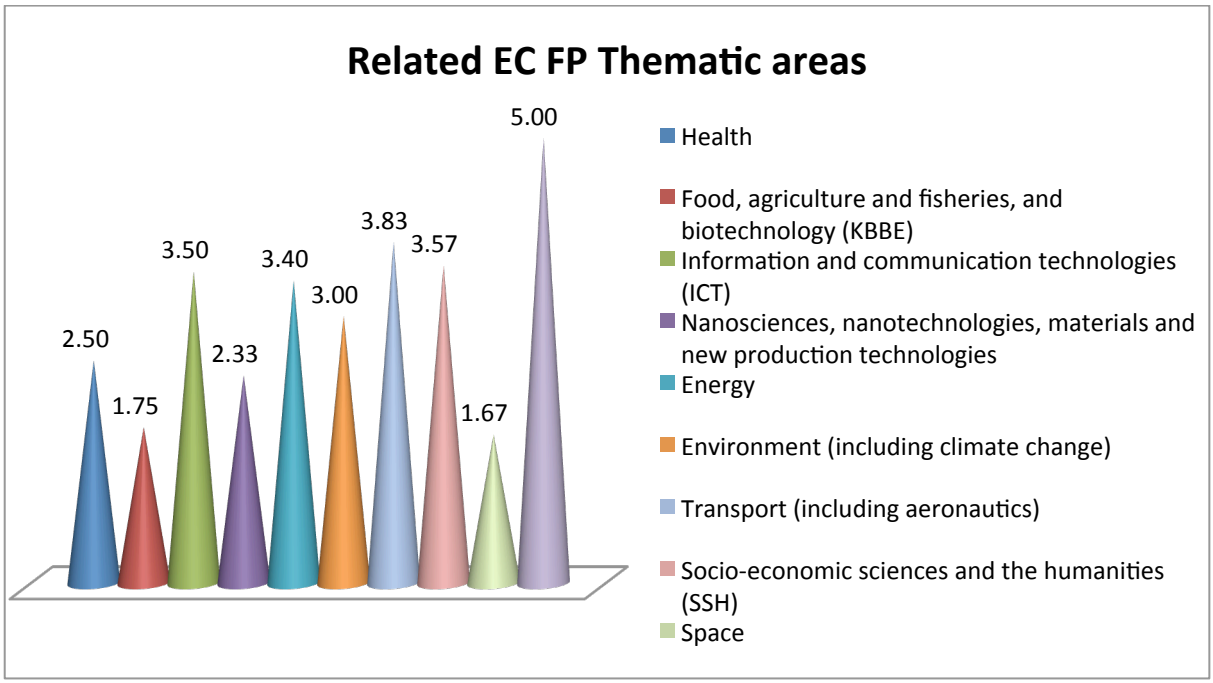
2.1.3 Context and domain coverage

The context of the FLAs was examined in relation to its funding/initiation, i.e. European Commission Framework Programme (EC FP) for Research and Innovation; European study detached from the EC FP; National study attached to a foresight or forward-looking programme; National study detached from a foresight or forward-looking programme; International FLA; Sub-national FLA; or Corporate FLA. Most of the security FLAs mapped were supported by the EC Framework Programme.

The domain coverage of the FLAs was mapped against the thematic priority areas of the EC as well as the FRASCATI and NACE taxonomies. In relation to the EC FP Thematic areas it is characteristic that the security FLAs were also linked to other thematic areas like SS&H, transport and ICT. Indeed the security area is closely linked to socio-economic issues in terms of

risk perception and social behaviour and (re)action to possible threats and risks. Moreover, technological developments as in the area of ICT play a crucial role as drivers for future security developments while at the same time they may also be considered as sources of insecurity raising certain ethical, legal and social issues. The strong linkages to the transport area reflect the importance of security research in (critical) infrastructures and interconnected networks, indeed an area of major importance for the EU. The examination of the related NACE categories repeats the importance of the ICT sector for EU security research.

Figure 4: Domain coverage of security FLAs

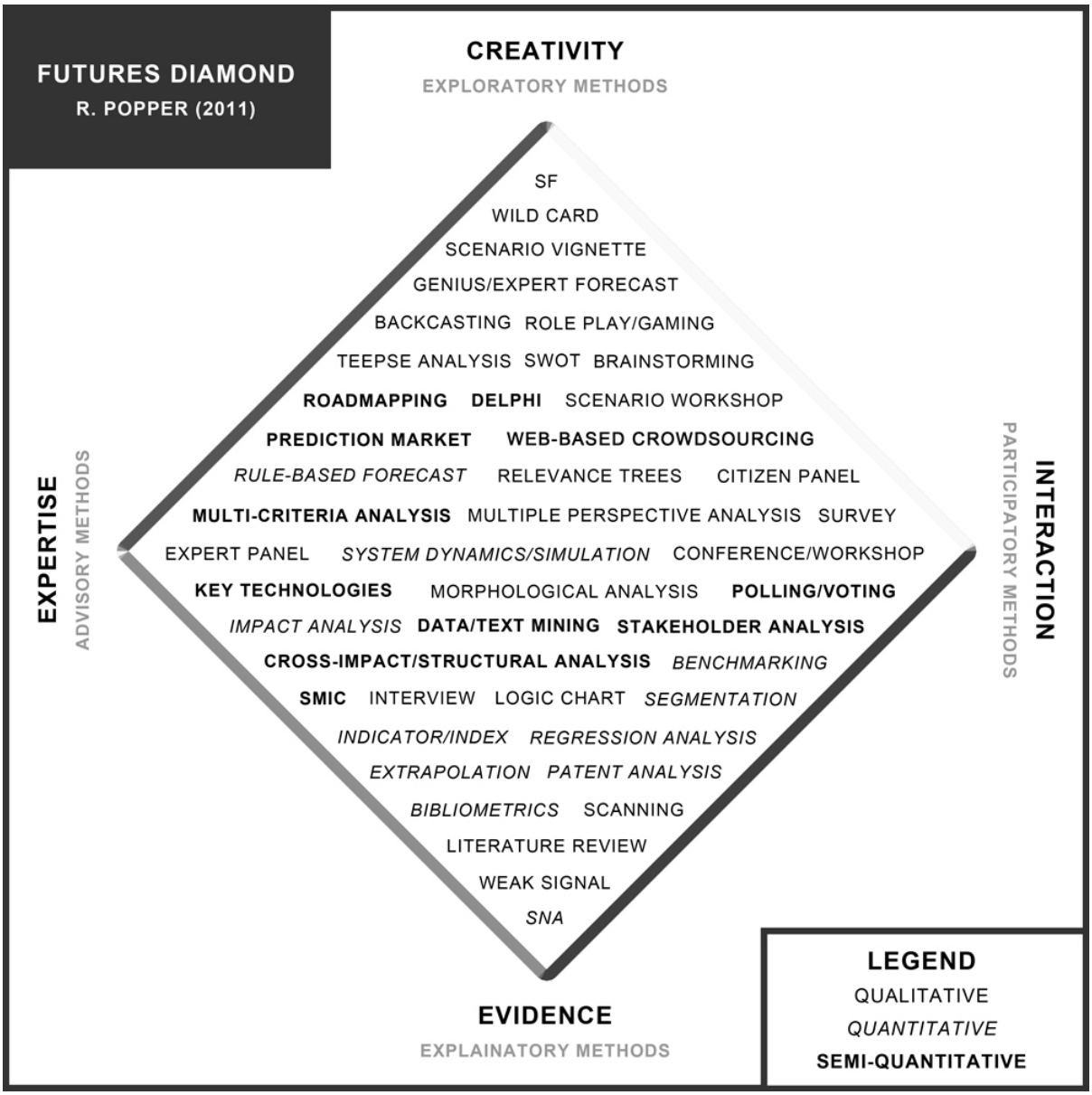


EFP mappers had the opportunity to choose from 1 to 5 stars to show relevance of aims to the specific FLA. The number shown on top of each bar is the mean of these scores.

2.1.4 Methods

The methods used include mainly qualitative options including 'brainstorming', 'conferences/workshops', 'interviews', 'literature reviews', 'scenario workshops' and 'surveys'. A couple of semi-quantitative methods are also used more sparsely however (Delphi surveys and web-based crowd sourcing).

Figure 5: The Futures Diamond



Source: Adapted from Popper (2008)

The methods applied draw mostly on expertise and experience, than creativity and interaction based on the Futures Diamond as illustrated above. They engage mainly academics and theme experts having the policy community as the main audience.

2.1.5 Territorial scope and time horizon

The territorial scope is in the vast majority supranational extending to the EU countries, while also covering some non-EU countries like USA (PATS) or the NATO alliance (Security Jam, 2012). Given that most of these FLAs are sponsored by the European Commission they are considered of high relevance to the EU.

The time horizon of most mapped security FLAS extends to 2020, 2030 or 2040, i.e. has in most case a medium-term perspective.[4]

2.2 Mobilising Futures - Results on FLA players

The mobilising phase of the SMART jigsaw refers to the FLA players. The indicators covered in the report in terms of FLA players are sponsors, target groups, public relations (PR) and marketing.

The First Annual Mapping Report (Popper and Teichler, 2011) noted that the mapping of FLA players would enable networking and cooperation between existing FLA communities, as well as the identification of methodology and domain experts in different countries around the world. Apart from this, the mapping of FLA players can help draw conclusions regarding the degree to which the target groups are extended from the usual suspects (i.e. academia and research, businesses and policy-makers). Regarding the PR and marketing conclusions can be drawn in terms of how much 'new' means are used beside more conventional ones (like printed material, websites and conferences).

2.2.1 Sponsors

Given that most of the security FLAs are EC FP funded projects it is not surprising that in most cases the sponsor is the EU.

2.2.2 Target groups

It is reminded that target groups are types of stakeholders or organisations that forward-looking activities aim to inform or influence. Target groups can be reached by either engaging them in the early stages of the FLA process (*scoping*, *mobilising* and *anticipating* futures) or by addressing them in the later phases (i.e. *recommending* and *transforming* futures). In EFP mapping the following target groups are considered (Popper and Teichler, 2011):

- *Public organisations* – including public corporations and national industries; government departments or ministries; government agencies; and parliaments.
- *Research and education organisations* – including: research funding organisations; public research organisations (non-HEI); private research and innovation support organisations; higher education institutions (HEI); and primary and secondary schools.
- *Private organisations* – including SMEs (e.g. consultancies and IT services); large and transnational companies; and associations representing commercial interests.
- *European Union* – including the European Commission; the European Parliament; and other EU bodies/agencies.
- *International agencies* (OECD, UNESCO, UNIDO, etc).
- *Non-governmental, not for profit, organisations* (NGO).
- *Media* – including the corporate and community/alternative press.
- *Civil society.*

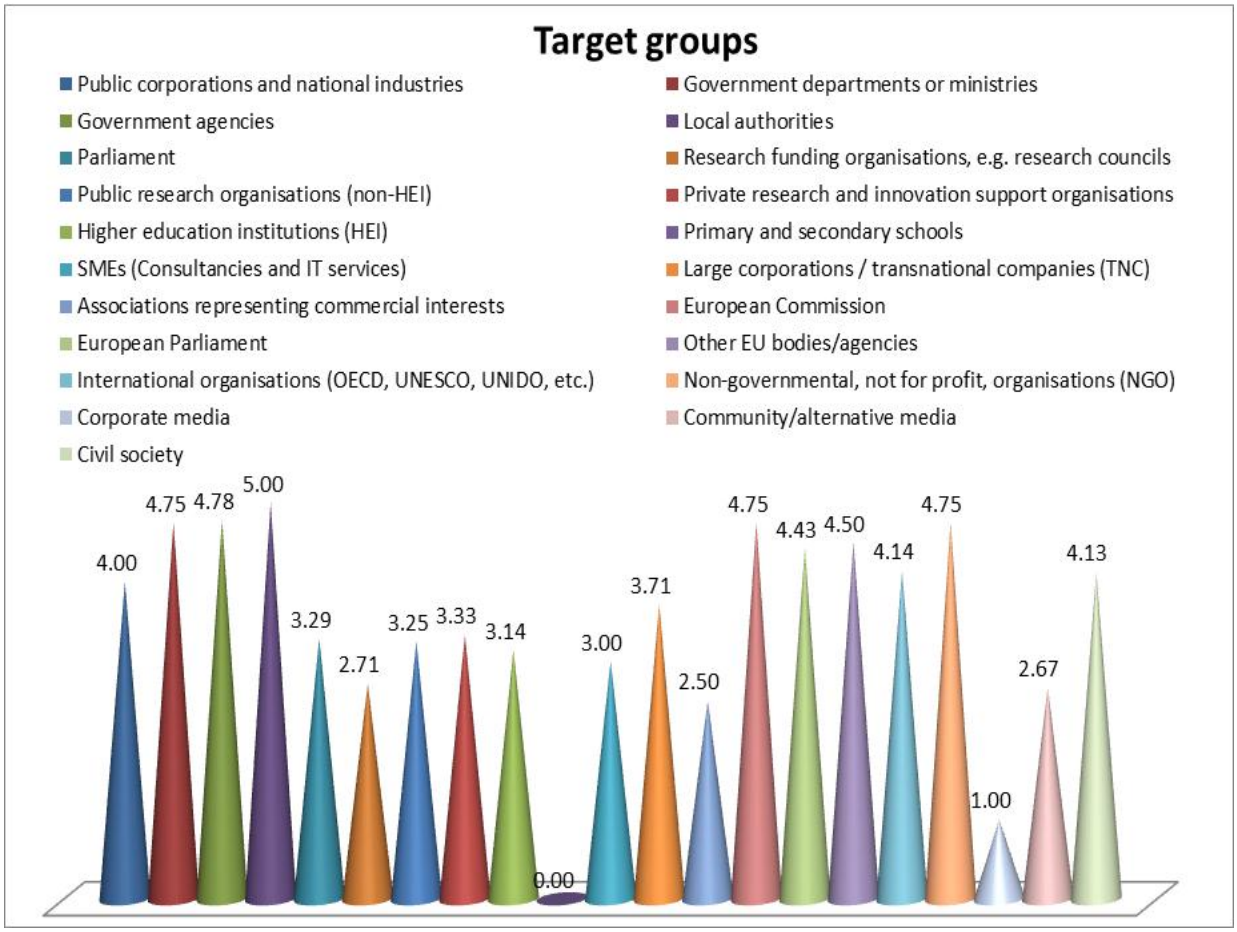
The main target groups of the security FLAs do not present any surprises nor do they go beyond the 'usual suspects'. These are public corporations, government departments and agencies and

[4] The risk/impact assessment studies do not usually have a specific time horizon.

local authorities and also the European Commission and the European Parliament, followed by other European EU bodies and international organisations (OECD, UNESCO, UNIDO, etc.) and NGOs. While the civil society is also considered an important target group, the corporate sector is interestingly much less considered as target audience.

The lack of corporate actors among the key target audience is surprising for two reasons. On the one hand, it is companies that own some of the most important and vulnerable security referents e.g. critical infrastructure or financial institutions and, on the other, the private sector marshals a significant part of the intellectual, administrative and financial resources to provide security. One does not need to think about the outsourcing of military functions to private military companies but merely about the importance of firms like Google, McAffee or Deutsche Telekom for cyber security.

Figure 6: Target groups of security FLAs



EFP mappers had the opportunity to choose from 1 to 5 stars to show relevance of aims to the specific FLA. The number shown on top of each bar is the mean of these scores.

2.2.3 PR and marketing

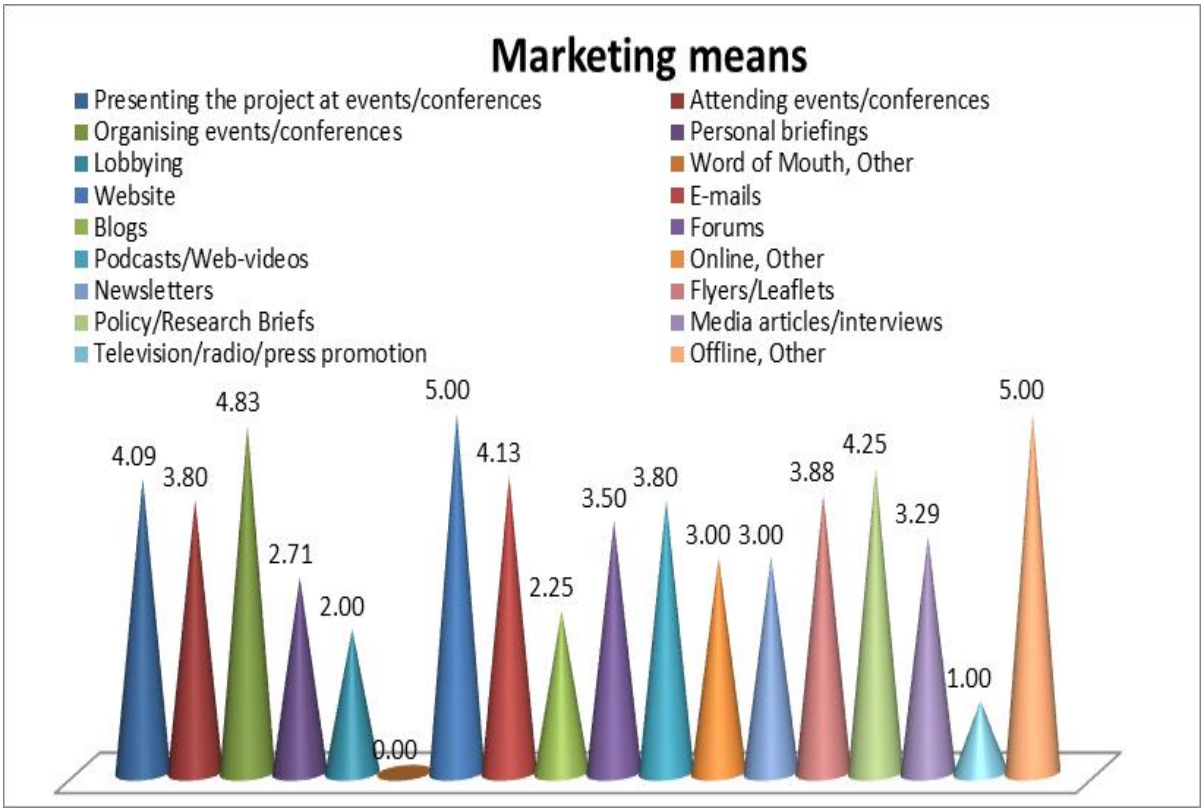
Common PR activities include: presenting the project at events/conferences organised by others; attending events/conferences organised by others; organising events/conferences; personal briefings; lobbying; etc. Marketing refers to online and offline means. By online we mean the use of websites, emails, blogs, web-discussion fora, web-videos/podcasts; while offline

refers to the use of newsletters, flyers/leaflets, policy/research briefs, media articles/interviews, television/radio/press promotion, etc. (Popper and Teichler, 2011).

The security FLAs used more conventional types of PR and marketing by mainly applying some of the so-called 'word of mouth' methods like presenting, organising and attending events and the usual 'on-line' methods like website and e-mailing lists. Some also printed newsletters and posters and established blogs while others also had papers printed in off-line media.

The tendency seems to be the use of a wide range of PR and marketing means across the different FLA groups irrespective of their specific focus, scope or type. Means of the 'word of mouth' and 'off-line' groups[5] seem to be most commonly used. On-line forums and podcasts are also used but to a lesser extent. Of the off-line means the production of policy briefs seems to be rising alongside newsletters and flyers.

Figure 7: Marketing means of security FLAs



EFP mappers had the opportunity to choose from 1 to 5 stars to show relevance of aims to the specific FLA. The number shown on top of each bar is the mean of these scores.

[5] 'Word of mouth' means: Presenting the project at events/conferences organised by others; Attending events/conferences organised by others; Organising events/conferences; Personal briefings; Lobbying. Off-line means: Newsletters; Flyers/Leaflets; Policy/Research Briefs; Media articles/interviews; Television/radio/press promotion.

2.3 Anticipating, Recommending and Transforming Futures - Results on FLA outcomes

The mapping of FLA outcomes is fundamental to access key information providing strategic intelligence for different policy areas and levels. However, there are specific challenges in this task. First, there is the issue of terminology. Although there is a more or less shared understanding of the terminology used in FLAs, there are cases where the term 'scenarios' for example is used to articulate specific 'visions' or to document the different development paths of quantitative indicators. 'Trends' are sometimes inter-changed with 'drivers', while there is little reference to 'megatrends' or 'grand challenges' as such in the FLAs documents[6].

The outcomes of FLAs are strongly dependent on the aims, rationales and specific focus of each FLAs. In this regard, a way to analyse outcomes is by examining their relation to specific rationales and scope of the FLAs. This approach is followed in the sections below.

At this point two other issues have to be noted as highlighted in the First Annual Mapping Report (Popper and Teichler, 2011). The first concerns the existence of different levels of sophistication in the mapping of FLA outcomes and results as these depend on whether the mapped FLAs are still ongoing or completed studies. Secondly, the time gap between the mapping and the completion of the mapped project is another factor influencing the precision of the mapping work: the longer the time that passed, the weaker are the memories of the interviewees and the greater the inability to find relevant documents and evidence.

2.3.1 Anticipating futures

Anticipating Futures refers to the "formal outputs" of FLAs which include: Visions, scenarios and forecasts; Critical and key technologies; TEEPSE drivers, trends and megatrends; SWOT and Grand Challenges; Wild Cards and Weak Signals (WIWE); Pathways and roadmaps; and Models and frameworks. (Popper and Teichler, 2011)

2.3.1.1 Drivers, Trends Megatrends and Grand Challenges

Not surprisingly, there is no clear separation between drivers, trends, and megatrends. It is also often the case that what is emphasised as megatrends or trends is also implicitly or explicitly linked to certain (grand) challenges. However, the analysis is not of a generic type but focuses on the security perspective. Some issues are mentioned in more than one group (as both trend and challenge for instance) while some clustering would also make sense. This is attempted in the following paragraphs.

Globalisation is a major driver of evolutions with significant implications for security. Globalisation is likely to raise the level of interdependence between states and individuals within the globalised economy. Resources, trade, capital and intellectual property are likely to rely on complex networks of physical and virtual infrastructure that are likely to be vulnerable to physical disruption or cyber-attacks by multiple actors. Consequently, increasing dependency on this infrastructure, and the global supply chains that underpin globalisation, will leave the global economy vulnerable to disruption. (DCDC Global Strategic Trends 2040)

---

6 This maybe because the 'grand challenge' rhetoric was not that intensely used at the time of the execution of the projects, some of which started around 5 years ago.

One of the main trends mentioned in the security FLAs is the **emergence of new centres of power** and the consequent **redistribution of global power**. (EU-GRASP, NIC Global Trends 2025) The emergence of new powers is first addressed as a key driver. Associated to this is the shift of power to Asia recorded as a major trend. In particular the world of 2030 will be diffusely multipolar and polycentric. Polycentrism will be accompanied by an economic power shift toward Asia, where over half of the world's population will be concentrated by 2030. China is projected to be the largest economic power and India will continue to rise. Both countries will face major structural challenges, however. Brazil may become a successful example of sustainable development during the next two decades. Russia and Japan will lose the great power status they enjoyed in the twentieth century. (ESPAS Global Trends 2030)

A constellation of rising middle powers, including Indonesia, Turkey, and South Africa, will become ever more prominent. (NIC Global Trends 2025) The international system that is likely to emerge as a result of all these shifts will probably mix balance-of-power politics and multilateralism, with states making issue-by-issue shifts and alliances. This will generate a higher level of unpredictability in international relations, and make it harder to attain a broad consensus even on matters requiring urgent global action. (ESPAS Global Trends 2030) This shift of global power is likely to result in a period of instability in international relations, accompanied by the possibility of intense competition between major powers as there will be several states and institutions competing for regional and global influence, cooperating and competing within the international community. (DCDC Global Strategic Trends 2040)

Redistribution of power on a global scale is addressed as a megatrend. Following the emergence of new powers this redistribution is marked by a move away from the United States (US) and Europe towards Asia and is also pushed by the urgency of global challenges (the financial crisis, climate change, maritime security, resource scarcity and population growth) (Security Jam 2012, NIC Global Trends 2025, DCDC Global Trends 2040)

The grand challenges addressed in the security FLAs are climate change, scarcities, global inequalities, changing demographics and migration.

Climate change has a central position in the analysis of trends and challenges, the focus being on the impacts from climate change. Temperature increases are likely to lead to significant environmental change that may, for example, include desertification in the Saharan margins and changes to rainfall distribution patterns within the monsoon belt of the Arabian Sea and South Asia. The frequency and intensity of extreme weather events will change, possibly with severe impact on low-lying coastal regions. Rapid glacial melt, particularly in the Himalayas, may exacerbate water management problems in China, India, Pakistan and Bangladesh. Disease carriers, such as malarial mosquitoes, are likely to spread into previously temperate zones. (DCDC Global Strategic Trends 2040)

Special reference is being made on the consequences of climate change affecting living standards and public safety by exacerbating water and food scarcity with environmental degradation expected to continue to provoke humanitarian disasters, including desertification and floods of increasing magnitude. The severest impact will be felt in China, South Asia and the Sahel, where millions of people will be displaced; but no region of the world will be spared. (ESPAS Global Trends 2030)

Scarcity in energy, food and fresh water resources is also separately addressed in relation to the social unrest and conflicts they may cause. The frequency, scale and duration of humanitarian crises are likely to increase. Many states, including China and India, are likely to become more dependent on food imports to feed their large and increasingly affluent populations. A shift in agricultural patterns and the distribution of grain growing areas, coupled with the rise in animal and plant diseases, is likely to disrupt food production, resulting in increased migration. However, improvements and efficiencies in agricultural production are likely to meet much of the increased demand, given likely scientific advances that develop high-yield, disease resistant crop strains, combined with better land usage and improved irrigation. The oceans will be further exploited for protein, raising the demand for fishing rights in previously inaccessible areas, such as the Polar Regions. (DCDC Global Strategic Trends 2040) Humanitarian crises due to water scarcity and related food and health emergencies may become recurrent, particularly in some parts of Africa. Competition for resources is likely to exacerbate tensions and trigger conflicts. Energy crises will heighten the sense that the world is entering an 'age of scarcity', putting the prevailing model of development into question. (ESPAS Global Trends 2030)

Inequalities of opportunities is another grand challenge due to globalisation and increased access to more readily and cheaply available telecommunications. This type of inequality is likely to be a significant source of grievance, possibly resulting in an increased incidence of conflict. However, states that experience lower birth rates and increased longevity are likely to benefit from a growing workforce and a falling dependency ratio. The result is a 'demographic dividend', which can produce a virtuous cycle of growth. (DCDC Global Strategic Trends 2040)

Demographic trends are also mentioned among the grand challenges as possible causes of tensions. Demographic trends may fuel instability especially in the Middle East, Central Asia and sub-Saharan Africa. The developing world will account for most of the growth, remaining relatively youthful, in contrast to the developed world and China, which will experience little population growth and undergo significant increases in median age. In the West, however, ageing is likely to lead to policies to employ the 'younger old'. This cultural shift may yield a second demographic dividend leading to a lower demand for migrant workers and decreasing the social welfare burden. (DCDC Global Strategic Trends 2040) The populations of several youth-bulge states are projected to remain on rapid growth trajectories. Unless employment conditions change dramatically in parlous youth-bulge states such as Afghanistan, Nigeria, Pakistan, and Yemen, these countries will remain ripe for continued instability and state failure. (NIC Global Trends 2025)

Nevertheless, populations in many affluent societies are likely to decline, encouraging economic **migration** from less wealthy regions. Environmental pressures, economic incentives and political instability will continue to drive population movement from afflicted regions. Conflict and crises will also continue to result in the displacement of large numbers of people. Such movement is likely to occur in regions of sub- Saharan Africa and Asia. (DCDC Global Strategic Trends 2040)

Health is another major issue among the trends examined by security FLAs with significant implication due to expected inequalities, movement of people and rising migration. By 2040, health will be recognised as a fundamental global issue. Average global life expectancy is likely to increase but access to healthcare is likely to remain unequal between the developed and developing worlds and, at the national level, between different socio-economic groups.

Dependence on international trade, relatively unconstrained movement of people, and high levels of legal and clandestine migration will minimise the opportunities to isolate outbreaks. (DCDC Global Strategic Trends 2040)

It is recognised that these trends and megatrends along with the challenges humanity is facing call for global responses. However **global initiatives** also hide a number of **gaps**. The ability of new constellations or 'hubs' of states to address grand challenges such as financial crises, climate change and resource scarcity to find shared solutions will be partial at best. There will be increasing pressure to reform multilateral institutions to reflect shifting power relations, including a drive towards greater inclusiveness. While the shift away from the Atlantic will be contested and may produce serious tensions, the overarching trend may well be towards convergence. It is likely that this shift in the global agenda will make consensus on international military interventions more dependent on a UN mandate than in the past. (ESPAS Global Trends 2030)

However, in a world characterised by the diffusion of power, meeting the challenges of human development will depend increasingly on **non-state actors**, be they private companies, non-governmental organisations (NGOs), or philanthropic institutions. Non-state actors, in particular national and transnational civil society networks and private corporations, will play a critical role in the coming decades. Their power and influence will be greater than that of many states, and may lead to new forms of governance and civic action. The devolution of power to federated states and regional and local authorities will continue and even accelerate. But not all contributions by private actors will be positive: extremist non-state actors are likely to present a threat to the well-being of human communities. (ESPAS Global Trends 2030)

The rising power of non-state actors vis-à-vis the state is a central theme examined from several perspectives. Concurrent with the shift in power among nation-states, the relative power of various non-state actors—including businesses, tribes, religious organizations, and criminal networks—is increasing. The global political coalition of non-state actors plays a crucial role in securing a new worldwide climate change agreement. In this new connected world of digital communications, growing middle classes, and transnational interest groups, politics is no longer local and domestic and international agendas become increasingly interchangeable. (NIC Global Trends 2025)

Main drivers for the empowerment of individuals are key developments in several spheres including the global emergence of the middle class, particularly in Asia, near-universal access to education, the empowering effects of information and communications technology (ICT), and the evolution in the status of women in most countries. (ESPAS Global Trends 2030)

In turn the impacts from the empowerment of individual and non-state actors are addressed. In democratic societies, new forms of protest and anti-establishment politics may emerge in response to a growing expectations gap, deepening income disparities, and the power shifts that are limiting the action of countries that have been used to acting as major global players. From the security perspective it is expected that over the next two decades the cyber sphere is likely to become an arena of conflict and tension between states of all political stripes, and also between individuals or private companies. It is likely that some governments will be more concerned with cyber security, control, surveillance and regulation than with protecting freedom of access. (ESPAS Global Trends 2030) Intrinsic to the growing complexity of the overlapping roles of states, institutions, and non-state actors is the proliferation of political

identities, which is leading to establishment of new networks and rediscovered communities. No one political identity is likely to be dominant in most societies by 2025. Religion-based networks may be quintessential issue networks and overall may play a more powerful role on many transnational issues such as the environment and inequalities than secular groupings. (NIC Global Trends 2025)

The examination of the **role of the individual** in future societies goes even further indicating the citizens of 2030 will be very much more aware that they are part of a single human community in a highly interconnected world. This may signal the rise of a new 'age of convergence.' Democratic aspirations will tend to be perceived as compatible with, and even as facilitating, a greater awareness of national and sub-national cultural identities. (ESPAS Global Trends 2030)

The **role of women** is also examined. Over the next 20 years the increased entry and retention of women in the workplace may continue to mitigate the economic impacts of global aging. Examples as disparate as Sweden and Rwanda indicate that countries with relatively large numbers of politically active women place greater importance on societal issues such as healthcare, the environment, and economic development. If this trend continues over the next 15-20 years, as is likely, an increasing number of countries could favour social programs over military ones. Better governance also could be a spinoff benefit, as a high number of women in parliament or senior government positions correlates with lower corruption. (NIC Global Trends 2025)

The **current economic crisis** is referred to as a driver that may reverse the trend of decreasing inequalities due to the emergence of a middle class in Asia, Latin America and also Africa. Overall, however, inequality will tend to increase and **poverty and social exclusion** will still affect a significant proportion of the world population. (DCDC Global Trends 2040) At the same time increasing social and economic pressures may undermine liberal institutions and the long-term prospects for greater democratization. (NIC Global Trends 2025)

Other trends refer to the main aspects of security that will attract attention in long-term strategic planning. These are proliferation (including by non-state actors), cyber security or instability emanating from failing states – humanitarian crises, piracy and organised crime – and the protection of natural resources and access to energy.

The **proliferation** of modern weapons' technologies will generate instability and shift the military balance of power in various regions. Nuclear weapons are likely to proliferate. Terrorist groups are likely to acquire and use chemical, biological and radiological or nuclear (CBRN) weapons possibly through organised crime groups (DCDC Global Strategic Trends 2040) but a major conflagration involving CBRN weapons is not likely to happen over the next two decades. (ESPAS Global Trends 2030, NIC Global Trends 2025)

Increasing dependence on ICT and reliance on space-based assets to receive or transmit information across the electromagnetic spectrum, will maintain the importance of **cyber security**. Attribution, intent and legitimacy of cyber-attacks will all be disputed. (DCDC Global Strategic Trends 2040)

The possibility of **inter-state conflict** cannot be discounted entirely. Looking ahead to 2030, the border tensions between China and India over water resources have the greatest potential to disrupt international peace. Conflicts are also foreseen due to current tensions between Algeria

and Morocco over the Western Sahara; the problems emerging as a result of the possible collapse of North Korea; and unresolved conflicts in Eastern Europe. **Tensions over raw materials** may also cause conflict and require new forms of crisis management. Intra-African and trans-regional **forced migration** due to economic factors, conflicts and environmental degradation will tend to grow. Wars fuelled by **nationalism and extremist identity** politics, and the associated dangers of mass murder and genocide, will be in the core security challenges of the coming decades. (ESPAS Global Trends 2030)

Despite the emergence of a possible 'age of convergence', **ideologically-driven conflicts** is another form to continue to exist. The social tensions caused by intrusive global culture are likely to be most acute amongst those who seek to maintain their indigenous and traditional customs and beliefs, and feel threatened by changes. This is likely to lead to an increasing number of individuals and groups, many of whom form around single issues that differentiate them from wider society, becoming marginalised and possibly radicalised. When such conditions exist, particularly when exacerbated by high levels of marginalisation and social exclusion, sections of the populace will develop grievances that may lead to extremism. (DCDC Global Strategic Trends 2040)

At the same time economic and social difficulties in some countries will lead to extremist identity politics and xenophobia. New ideologies will emerge, driven by religion, ethnic differences, nationalism, inequality or a combination of these factors. Those communities that fail to integrate are likely to remain reservoirs for resentment. (DCDC Global Strategic Trends 2040, NIC Global Trends 2025)

Urbanisation is also seen as an important trend. By 2040, around 65%, or 6 billion, of the world's population will live in urban areas, attracted by access to jobs, resources and security. The greatest increases in urbanisation will occur in Africa and Asia. As up to 2 billion people may live in slums, these areas are likely to become centres of criminality and disaffection and may also be focal points for extremist ideologies. Rapid urbanisation is likely to lead to an increased probability of urban, rather than rural, insurgency. (DCDC Global Strategic Trends 2040)

In addition, **megacities** are also highlighted as possible sources of conflicts as well as important future players. By 2030, the fifty greatest megacities in the world will concentrate more resources than most small and middle-income states, and they will demand more autonomy and exert greater power, even taking on a more prominent international role. Preserving humane living conditions in the world's megacities will be the major challenge facing some states. Cities will also absorb most national security resources. (ESPAS Global Trends 2030)

Trends in **innovation and technology** are also being examined especially in providing solutions to the major trends and challenges as those mentioned above. Technology will provide partial solutions for both adapting to, and mitigating the effects of, climate change. However, it is unlikely that, by 2040, technology will have produced low emission energy sources capable of providing the majority of the energy demanded. Nevertheless, advances in carbon capture technology are likely to be significant, allowing fossil fuel usage to continue in a limited emission regime, with particular expansion in the use of coal. Despite this, resource competition, carbon pricing, increased energy demand and the limitations imposed by climate change are likely to increase the cost of fossil fuels, stimulating the development of cleaner, renewable energy solutions and nuclear power. (DCDC Global Strategic Trends 2040) The pace

of technological innovation will be key to solving such challenges. However, even with a favorable policy and funding environment for biofuels, clean coal, or hydrogen, the transition to new fuels will be slow. (NIC Global Trends 2025).

The most significant **innovations** are likely to involve sensors, electro-optics and materials. Application of nano-technologies, whether through materials or devices, will become pervasive and diverse, particularly in synthetic reproduction, novel power sources, and health care. Improvements in health care, for those who can afford it, are likely to significantly enhance longevity and quality of life. Advances in robotics, cognitive science coupled with powerful computing, sensors, energy efficiency and nano-technology will combine to produce rapid improvements in the capabilities of combat systems. (DCDC Global Strategic Trends 2040)

However, from a security perspective, technology will also facilitate the organisation of protests and high impact terrorist attacks. The future global environment will be defined by physical, social and virtual networks. The physical system will consist of complex interconnections, including extensive resource pipelines, communication cables, satellites and travel routes. The virtual networks will consist of communications servers linking individuals and objects, many of which will be networked through individual Internet Protocol (IP) addresses. Avenues for protest, and opportunities for new and old forms of crime, will emerge and may allow hostile groups to form and rapidly create effect. (DCDCD Global Strategic Trends 2040)

In terms of **defence technologies** many states are likely to develop ballistic and cruise missiles capable of delivering CBRN weapons, as well as conventional payloads. Ballistic Missile Defence (BMD) and other air defence technologies may mitigate some of the risks. (DCDC Global Strategic Trends 2040) The majority of the technological breakthroughs are likely to be driven by the commercial sector, although technological adaptation in defence will continue at a rapid pace. Nonlethal, Directed Energy Weapons (DEW), space and cyber technologies will be available to a wide variety of actors, both state and non-state. (DCDCD Global Strategic Trends 2040)

Finally, the growing demand is recognised for multilateral policies in the global and regional arenas for an increasing number of issues from the fight against climate change to disease control. There is, therefore, need for more multilateralism and, arguably, for a larger European role. (EU-GRASP)

2.3.1.2 Visions, scenarios and forecasts

Visions are not that common in the security FLAs. There are only two cases expressing a shared vision of European security, i.e. FORESEC – although it is more in relation to the concept of security than a particular vision on how European security should develop - and a vision on integrated border management and critical infrastructure protection (STRAW)

Scenarios in security FLAs have a particular role. They are usually reflections of future states of the world in the event of particular threats or risks being materialised. Hence, there are scenarios about future regional conflicts; terrorism; WMD proliferation; energy security and climate change; severe human rights violations; migration. (EU-GRASP) Other examples include an earthquake inside or outside the EU; critical infrastructure failure: energy, telecom, ICT; terrorist action – CBRN; civil war; large-scale influx of refugees to EU. (ACRIMAS)

Box 1 - FORESEC vision of European security

FORESEC suggests that European security could be viewed as a concept with different dimensions. The key dimensions for understanding European security are: The first dimension, is the continuum between internal and external security. A distinctive feature of the security landscape in Western Europe after the end of the Cold War is that the division between internal and external security has become increasingly obsolete. Then there is the dimension of civilian and military security. The dimension of state, societal and individual/human security highlights that there is an increased focus on the citizen as the object of security. In the dimension concerning national, regional and global security, where a clear trend towards emphasis on regional security can be distinguished. A further dimension emphasises the role that societal resilience and the private sector play next to governments in providing security. Finally, the analysis of the contents of research being conducted under the early EU security research activities highlights the fact that this research tends to take security as a norm and a fundamental value. Since PASR there has been increasing reflection on the impact of security technologies with regard the fundamental freedoms and rights of individuals.

Other scenarios are of a more specific threat nature (FESTOS). These include:

- Cyber insects attack - As artificial bees replace extinct bee populations, the former get out of control attacking humans. This results in panic, great suspicion, a slump of the agro-food industry and suspicion about anything robotic;
- The Genetic Blackmailers - As individual genome analysis becomes accessible, affordable and quick information about a person's DNA can be easily obtained by other individuals or organisations. This poses severe risks for privacy and raises ethical issues;
- At the Flea Market - Everyday intelligent nanotechnology-based products can be set to self-destruct with a wireless signal. As a result local craftsmen benefit from the collapse of high-tech devices, normal economic life falters with flea markets flourishing due to skyrocketing demand for non-nano equipment.
- We'll change your mind - A terrorist group uses a virus to change the behaviour of a portion of the population for a certain time. An inaudible acoustic virus is able to influence the mind of infected people in ways controlled by emitter of the virus.

Finally, there are also cases where more holistic scenarios are developed following the more conventional concept of scenarios in foresight studies. For instance, one regards SANDERA where scenarios are reflecting different degrees of integration between EU research and defence policies. Another one regards certain states of world order (FORESEC) as presented in the following box.

Box 2 - FORESEC set of scenarios

Multiple Messes

• Competition and lack of trust between the leading world powers • Weak economic growth due to the effects of Climate change and protectionism • Armed conflicts and mass migration in EU's wider neighbourhood, caused by environmental degradation and struggle for resources • Violent radicalisation within the EU in immigrant populations and social groups hit hard by the weak economy • Privacy-invading security measures are found acceptable to the EU population because of the perceived insecurity • Security is mainly seen as a concern for governments, which makes large-scale orders for development and manufacturing to big companies • A robust critical infrastructure in the EU, generally seen as a result of research within the EU framework programmes • European cohesion is strong at state level and the EU has an effective decision-making structure in line with the Treaty of Lisbon • The situation in the Middle East is extremely tense and it is believed that Iran has nuclear weapons • Energy security is a problem as EU is very dependent upon producer countries • Russia has a strong and centralized political leadership and is a major energy exporter to the EU"

Euromerica

• US and EU working close together to further liberal democracy, primarily using soft power and diplomacy • Medium economic growth and rapid innovation and industrial pattern changes • Positive political and social development in EU:s wider neighbourhood but considerable environmental problems lead to strong migration push • Innovative public/private partnerships in the social domain lead to inclusive welfare in EU member states • Low acceptability of security measures in the EU caused by the strong emphasis on human rights and low threat levels • European cohesion is strong both between Member States and social groups and the EU has a decision-making structure in line with the Treaty of Lisbon • Vulnerable critical infrastructure in EU due to growing complexity and interlinkages of the systems • A sustainable political solution for the Middle East has been mediated. As a part of the deal, Iran gave up their nuclear weapons ambitions. • A diversified energy supply for the EU and a home-grown renewable energy capacity • Strained relationship with an increasingly authoritative Russia, caused by the US+EU emphasis of human rights"

Web of Security

• US and EU engaged in a Global struggle against violent extremism and terrorism • Medium economic growth • Cooperation with Russia over matters of mutual concern • Mass migration in EU's wider neighbourhood caused by armed conflict and environmental degradation • Negative feelings among some of the European citizens with links to the main scenes of conflict involved in the Global struggle • Strains between EU members states, but willingness to delegate power for security matters to the European level • Terrorist attacks and natural catastrophes have shown the vulnerability of the critical infrastructure in the EU • The situation in the Middle East is problematic with more or less regularly recurrent smaller regional proxy wars • Lack of affordable energy supplies in the EU • Ineffective decision-making structures in the EU makes many consider EU a "lame duck" (although not with regard to security) • Far-reaching and privacy-invading security measures are found acceptable due to high levels of external and internal threats"

In the security FLAs mapped there were hardy any forecasts in the classical sense, i.e. quantitative statements of the outcomes of particular events or trends in a specific time in the future. However, forecasts of a more qualitative nature were retrieved mainly from the studies examining global trends and the risk assessment studies. Naturally, these relate to some of the major trends presented in the previous section, although some of them are quite specific in examining the **nature of future conflicts**.

More specifically, state and non-state actors will seek to combine conventional, irregular and high-end asymmetric methods concurrently, often in the same time and space and across the combined domains of the air, land, sea, space and cyberspace. **Conflict** is likely to involve a range of transnational, state, group and individual participants who will operate at global and local levels. In some conflicts, there is likely to be concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder. These forms of conflict will transcend conventional understanding of what equates to irregular and regular military activity. States will increasingly sponsor proxies, seeking to exploit gaps in the international system while minimising state-on-state risks. The range of threats will diversify, as technology and innovation opens up novel avenues of attack and adaptive adversaries exploit opportunities. (DCDC Global Strategic Trends 2040) **Terrorism** is unlikely to disappear by 2025, but its appeal could lessen if economic growth continues in the Middle East and youth unemployment is reduced. (NIC Global Trends 2025) The **CBRN threat** is likely to increase, facilitated by lowering of some entry barriers, dual purpose industrial facilities and the proliferation of technical knowledge and expertise. The likelihood of nuclear weapons usage will increase. (DCDC Global Strategic Trends 2040)

The incidence of **armed conflict** is likely to increase underpinned by an unstable transition to a multi-polar world that allows old and new state rivalries to emerge; widespread global inequality that heightens associated grievances; population increases, resource scarcity and the adverse effects of climate change that combine to increase instability; and the increased importance of ideology. (DCDC Global Strategic Trends 2040) Military operations are likely to continue to result in casualties and face the challenge of demonstrating legitimacy to sceptical public audiences. Influence activity, the battle of ideas, and perceptions of moral legitimacy will be important for success. Where instability affects national and multilateral interests, there is likely to be a requirement to provide support for legitimate governance structures and for stabilisation operations.

Associated to the nature of conflict was the issue of conflict governance. **Conflict governance** will require a multi-actor and multi-level approach. Multilateral military activity is likely to protect globalisation, including protection of global supply chains and space-based infrastructure. State interdependence will give most conflicts, wherever they occur, a global dimension. The changing balance of power is likely to deter military intervention by major powers outside their spheres of influence, without widespread multilateral agreement, which is likely to reduce the latitude for discretion. Persistent, complex problems will require the integration of all levers of state power, both across government and among partners and allies. (DCDC Global Strategic Trends 2040)

New alliances and partnerships will form and established ones will be adapted to meet the breadth and depth of the challenges. For European powers, the North Atlantic Treaty Organization (NATO) is likely to remain the defence organisation of choice. Competition for

resources will increase the geostrategic importance of certain regions such as; the Asian Meridian, the wider Middle East and the Polar Regions. (DCDC Global Strategic Trends 2040)

At the same time **soft power** will be utilised in facilitating the achievement of political goals. All elements of power are likely to be used by a broader spectrum of actors and agencies, including organised criminal, terrorist and insurgent groups. Nonetheless, while traditional levers of power will continue to form the basis of statecraft, it is unlikely that the military instrument alone will be decisive. (DCDC Global Strategic Trends 2040)

As expected **demographics** is also another issue studied in global trends but from an interesting perspective examining the need for humanitarian intervention. Out to 2040, the demographic profiles of societies will change with the developing world accounting for the majority of population growth and representing 85% of the global total. However, limited economic development and cultural norms will persist, sustaining high fertility rates in regions such as sub-Saharan Africa, parts of the Middle East and Asia, and specifically in countries such as Afghanistan, Syria, Yemen and Pakistan. In contrast, Europe, Japan and eventually China and Latin America are likely to face the problems of an ageing and declining population. However, the long-term decline in fertility rates experienced by the most developed states is eventually likely to be halted, or even reversed, as societal norms change. Clear moral cases that invite humanitarian intervention will persist. (DCDC Global Strategic Trends 2040)

The role of **education** is also marked as the globalised economy becomes increasingly dependent on knowledge-based industries, creativity and innovation. Global access to education will remain variable, though, although ICT based initiatives are likely to improve basic skills in numeracy and literacy. This implies possible resentment as those who do become better educated may suffer frustration if they continue to experience inequality of opportunity based on their physical location, culture or language. (DCDC Global Strategic Trends 2040)

2.3.1.3 Wild cards and weak signals

Security FLAs are particularly interested in wild cards. As presented above several of the scenarios developed in the security FLAs were representations of a future state of affairs in case a certain threat or risk is materialised. In this regard these scenarios can also be considered as wild cards even though they were not titled as such in the project documentations.

One particular FLA with special reference to certain wild cards as presented in the following box. It is interesting to see that even positive events like finding the cure for cancer or a new energy source can have serious implications on changing the current state of affairs and thus causing instability and tension. Another relevant example is the set of wild cards included in the NIC Globals Trends 2025 as shown in Box 4.

Box 3 - DCDC Global Strategic Trends 2040 identified a list of wild cards

Collapse of a Pivotal State - The sudden collapse of a pivotal state would threaten regional and global stability. For example, the descent into instability of a major hydrocarbon exporting state, such as Nigeria, Iran, Saudi Arabia or Russia, would have local and regional consequences, disrupting global energy supplies. This would affect global energy markets causing widespread economic, social and political dislocation. Similarly, if internal tensions caused instability within China the global economy could be disrupted by the simultaneous drop in demand for raw materials and reduced supply.

Cure for Ageing - The development of a treatment that could prevent or cure the effects of ageing would have a significant impact on global society. Initial access to such an advance could be highly unequal and only be available to wealthier members of society, mostly in the developed world. The whole fabric of society would be challenged and new norms and expectations would rapidly develop in response to the change.

New Energy Source - A novel, efficient form of energy generation could be developed that rapidly lowers demand for hydrocarbons. For example, the development of commercially available cold fusion reactors could result in the rapid economic marginalisation of oil-rich states. This loss of status and income in undiversified economies could lead to state-failure and provide opportunities for extremist groups to rise in influence.

Collapse of Global Communications - Failure of the global communications system could occur for a variety of reasons; for example the destruction of satellites following an orbital electromagnetic pulse detonation or solar flare, or the complete overload of the global ICT infrastructure. Such an event is not without precedent. Such a collapse would cause trade, commerce and the Internet to grind to a halt. Military operations dependent on the availability of communications networks would also be put at risk. Remaining bandwidth would see intense competition for access.

External Influences - These include a highly lethal pandemic, a geological or meteorological event of unprecedented scale, such as the eruption of a super-volcano, or the discovery of non-terrestrial intelligent life. In the military domain, the development of a new, as yet unforeseen capability that allows one state to exercise technological dominance over others would have a significant impact on the strategic context. Potential examples could include; quantum decryption, whole-scale application of nano-technology, biotechnology weapons or advanced robotics. This could ultimately result in the defeat of a Western military force on the battlefield in a 'maxim gun' moment, against an adversary who has the technological advantage over the West.

Box 4 - NIC Global Trends 2025 list of wild cards

Winners and Losers in a Post-Petroleum World - The geopolitical implications of a shift away from oil and natural gas will be immense. Saudi Arabia will absorb the biggest shock, as its leaders will be forced to tighten up on the costs of the royal establishment. The regime could face new tensions with the Wahabi establishment as Riyadh seeks to promote a series of major economic reforms—including women's full participation in the economy—and a new social contract with its public as it tries to institute a work ethic to accelerate development plans and diversify the economy. In Iran, the drop in oil and gas prices will undermine any populist economic policies. For Iraq, emphasis on investing in non-oil sectors of its economy will increase. Outside the Middle East, Russia will potentially be the biggest loser, particularly if its economy remains heavily tied to energy exports, and could be reduced to middle power status.

A Non-nuclear Korea? - A new, reunified Korea struggling with the large financial burden of reconstruction will be more likely to find international acceptance and economic assistance by ensuring the denuclearization of the Peninsula, perhaps in a manner similar to what occurred in Ukraine post-1991. A loosely confederated Korea might complicate denuclearization efforts. Other strategic consequences are likely to flow from Korean unification, including prospects for new levels of major power cooperation to manage new and enduring challenges, such as denuclearization, demilitarization, refugee flows, and financing reconstruction.

Potential Emergence of a Global Pandemic - If a pandemic disease emerges by 2025, internal and cross-border tension and conflict will become more likely as nations struggle to control the movement of populations seeking to avoid infection or maintain access to resources. Experts consider highly pathogenic avian influenza (HPAI) strains, such as H5N1, to be likely candidates for such a transformation, but other pathogens—such as the SARS coronavirus or other influenza strains—also have this potential. If a pandemic disease emerges, it probably will first occur in an area marked by high population density and close association between humans and animals, such as many areas of China and Southeast Asia, Under such a scenario, inadequate health-monitoring capability within the nation of origin probably would prevent early identification of the disease. Slow public health response would delay the realization that a highly transmissible pathogen had emerged. Waves of new cases would occur every few months. The absence of an effective vaccine and near universal lack of immunity would render populations vulnerable to infection.

2.3.1.4 Models and analytical frameworks

It is remarkable that several security FLAs either of the foresight or the assessment type contain a sophisticated model referring to conceptual or causal relationships. Thereby every project makes an important conceptual contribution to the scholarly debate in the security field, albeit with a concrete link to practical problems. Hence, the texts are a particularly fruitful source for further refinement and debate.

More specifically the FLAs mapped produced several conceptual frameworks to analyse the abuse of technology, to understand attitudes towards control of knowledge, to organise operations and to categorise certain trends and threats:

- Framework to analyse the abuse of technology - The framework distinguishes three types of the abuse of technology: technologies that enable misuse such as the internet; technologies that are harmful; and technologies that can harm unintentionally. (FESTOS)

- Typology of attitudes towards the control of knowledge - The typology distinguishes three groups of academics according to their attitude towards control and prevention of their work: ambivalent, control oriented and liberal. (FESTOS)

- Operational Fields Matrix - The matrix has 2 dimensions: level of action with the ends of Global vs. sub-state and the other being mandatory/coercive vs. voluntary measures. (FESTOS)

- Taxonomy on Trends, Drivers, and Threats - Taxonomy of threats consists of risk with its likelihood and impact. The latter two are increased or decreased by drivers and trends. Depending on the vulnerability the referent object will be damaged or hurt. (FORESEC)

Box 5 - FORESEC model for risk analysis

Certain analytical frameworks were also developed such as the analytical model supported by STRAWiki. This is an active technology tool to monitor what is relevant in the security domain in terms of knowledge, experience and stakeholders, and deliver this information to the right audience at the right time. This is supported by a technology watch portal, a semantic search engine and an own wiki (STRAWiki). In addition, a common framework for the analysis of critical road infrastructure objects (bridges/tunnels) or road transport networks was developed with regards to their importance within the European transport network. (STAR-TRANS, SERON)

A generic system architecture was developed with relevant functionalities for hazard identification to model the energy networks. (EURACOM) The architecture framework is based on the enterprise architecture paradigm, however primarily used as descriptive framework, describing the European energy environment.

PATS also developed a privacy accountability model. This included a set of activities (dimensions) that should be undertaken by security organizations in order to become privacy-accountable entities. It provided the basis for privacy branding through which security organizations might communicate privacy accountability and responsibility to citizens. The

activities included a) planning, awareness building, conceiving and strategizing related to privacy (reflexivity), b) making privacy-related information available to the public, c) exercising two-sided communication with stakeholders, including citizens, on issues of privacy (communicability), d) changing the behaviour of security organizations with respect to privacy, and e) evidencing and verification of privacy accountability (testability).

Finally, a decision support system is provided to end users of security investments (DESSI). The system gives insight into the pros and cons of specific security investments. It is useful for public authorities, developers of security solutions, commercial enterprises and for social organizations that can use the DESSI tool to make their own comprehensive assessment as an input to strategic discussions or public debate.

2.3.1.5 Key and emerging technologies

One might expect that key technologies would be a major outcome in security FLAs drawing on the experience from more traditional security FLAs originating in the defence sector (e.g. Ministries of Defence, defence think tanks). However, this is not the case in the security FLAs mapped as only two resulted in lists of future emerging technologies. This fact can be explained by the different nature of FLAs mapped with the importance attributed to the engagement of a broad variety of stakeholders and the different national perspectives that come to play in many EC FP funded projects.

Box 6 - FESTOS emerging technologies and potential threats associated to them

Cyborg insects and swarm robotics - Swarm robotics is a novel approach to the coordination of a large number of robots, inspired mainly by insects, which show how large numbers of simple individuals interact to create collectively intelligent systems. Researchers envision that robots will be mass-produced and programmed for various tasks such as surveillance, micro-manufacturing, cleaning or medicine. SIMBION, REFRACTO

Internet of things and ambient intelligence - Internet of things' (IoT) means a network of everyday objects such as food items, home appliances, clothing as well as various sensors that will be addressable and controllable via the Internet. IoT is related to the vision of Ambient Intelligence where people are surrounded by interconnected devices that are embedded in their surroundings and easily accessed via intuitive interfaces. Computers are everywhere but recede to the background, being invisible and seamlessly responding to the needs of individuals.

Molecular manufacturing - Materials that can be programmed to be self-assemble, after their shape and physical properties to perform a desired function and then disassemble after use or in response to user input or autonomous sensing. Known also as 'claytronics' or 'infochemistry' this emerging technology field combines theory of information, chemistry and progammability to build information into matter.

Metamaterials; Invisibility Cloaking - Nano-structured materials with negative refractive index. Can make objects invisible or appear as other objects.

Smart phone mash-up - Smart phones that are combined with new features such as GPS receivers, cameras and internet connectivity and can interact together or with internet services providing new functions for surveillance, data processing, observation or control, making a mobile phone an extremely potent device.

Box 6 - continued - FESTOS emerging technologies

Cloud computing - Cloud computing involves the provision of dynamically scalable and often virtualised resources as a service over the Internet. Providers deliver business services online which are accessed from a web browser, while the software and data are stored on servers, i.e. 'in the cloud'. Customers 'consume' the resources as services and pay only for the resources they use.

Synthetic biology - Synthetic biology involves the large-scale rewriting of the genetic codes to create metabolic machines with singular purposes. The vision is to develop synthetic biology into an engineering discipline with similarly standardised parts. Hence, synthetic biology means the in vitro of natural organic agents and combinations thereof from basic building blocks that are programmable like computers and that could function as tiny machines.

Nanotechnology-enabled brain implants - Various biomedical devices implanted in the central nervous system could control motor disorders or translate wilful brain processes into specific actions by the control of external devices.

2.3.1.6 Pathways and roadmaps

On a similar note, the security FLAs mapped did not result in specific pathways and (technology) roadmaps as one might expect. There was only one case (ACRIMAS) that developed a roadmap for an upcoming demonstration project within the area of crisis management as the Phase II of the ACRIMAS project. This roadmap would elaborate a systematic development process for crisis management systems, procedures and technologies in Europe, to be implemented within the demonstration project. The process aims for gradual evolvement of crisis management capabilities through demonstration and experimentation activities, transfer of related knowledge between stakeholders and by promoting an environment for co-development of crisis management technology and methodology where users, providers and researchers work together.

Overall, the main 'anticipation' outcomes of the FLAs mapped fall into the groups of trends, challenges, scenarios, and models rather than key technologies or roadmaps. The result is hardly a surprise given the aforementioned aims and rationales that emphasised the transformation of existing paradigms and the engagement of stakeholders and decision-shapers.

2.3.2 Recommending Futures

Recommendations from FLAs may fall into the following categories: Policies and actions; Initiatives and actors; Appropriation and dissemination; Investments and training; Alliances and synergies; (FHS) research. Based on the analysis of the security FLAs mapped almost all projects[7] focus in their recommendations on policy action and on future research.

The policy recommendations usually address the primary target audience according to the FLAs' scope and territorial coverage, i.e. policy-makers at national but mainly EU or international level. They may also correspond to the specific scenarios developed like in the case of SANDERA shown below.

[7] This excludes the assessment FLAs which usually produce "anticipating futures" types of outcomes and do not go further into the "recommending futures" types of outcomes.

Box 7 - SANDERA policy recommendations

Policy for scenario "Indifference" - Enhance strategic policy intelligence capacity in order to move towards a world of "indifference" between ERA and defence research and innovation in 2030. Even if the two policy domains (research and security) remain largely indifferent to each other, policy makers in both fields should carefully observe the developments in the respective other domain. ERA and defence policy makers should install an "early warning system" of change in this area and the consequences this might entail for ERA.

Policy for scenario "Integration" - Develop a shared vision and set common goals in order to move towards a world of "INTEGRATION" in 2030. In a first step, this discourse should focus on the European level and involve all relevant European agencies and initiatives (EDA, ESA, FRONTEX, EUROPOL, EUROJUST), the Commission (DG Research, High Representative for Security) and representatives from the Council Secretariat and the Council itself.

Policy for scenario "Cooperation" - Deepen the existing dialogue. There are a number of potential governance frameworks for cooperation such as ad hoc cooperation between ERA agencies and national bodies, or an institutional framework for cooperation based on an ESRIF-like approach. In this effort the common areas of interests should be identified while the differences in the rules governing civil and defence research should be mitigated.

Policy for scenario "Competition" - Develop policy goals based on the principles of human security in order to move towards a world of "COMPETITION" in 2030. The EU would deliberately abstain from any role in the defence research field and instead stress the civilian character of the Union's science and technology policy.

PATS policy alternatives to promote privacy accountability and privacy branding practices include incentives (top-down developed by governments or bottom-up developed by NGOs for example), regulations and self-regulation alternatives, and influencing the adoption of privacy branding. PATS also produced preliminary recommendations on how to promote privacy accountability and branding among security organizations in the countries covered by the study. In addition recommendations are produced to promote privacy accountability and branding practices at the European level in combination with the General Data Protection Regulation which may serve as a guideline for the security industry for co-regulation and privacy branding.

Other types of recommendations are more holistic in nature but still keep the security perspective at their core while addressing a number of grand challenges like in the field of energy, the environment or migration. This is the case of FORESEC, EU-GRASP or the NATO study (Security Jam, 2012) for example.

FORESEC recommends:

- To develop an EU energy security strategy - Energy policy is still driven by national-level approaches which stand in the way of a common energy strategy. A common energy strategy on subsidies for renewable sources would help to diversify energy supply. Europeans should focus on fostering relations with new and potential energy suppliers and transit countries.

- To reduce emissions and protect the environment - Work should be conducted from a joined-up economic and political perspective so that the security aspects of energy issues are incorporated into areas that are beyond, for example, the immediate scope of current security research programmes. For instance, research to reduce the effects of emissions on the environment can contribute to mitigating energy security risks by reducing external dependencies, helping with indigenous production and reducing the impact on the environment which has knock-on security impacts.

- To deal with security aspects of migration and changing demographic patterns

- To promote dialogue with the security and intelligence services across the EU - A dialogue with the security and intelligence services across the EU would be a useful input into the formulation of counter-terrorism legislation at the EU level.

- To increase public awareness of environmental risks - Increased communication and interaction between EU member states should be actively supported and encouraged. Similarly, communications between security / environmentally oriented civil-society organisations and the environmental and security policy communities within and between EU member states, and other European countries, should be supported.

- To reduce vulnerability of critical infrastructure - Critical infrastructure vulnerability might best be reduced by combining macro level efforts such as horizon scanning and policy planning with prioritized micro level actions. This will need to start with threat assessments combined with impact/vulnerability assessments where steps have been taken to protect assets. In this way, progress towards mitigation can be measured and further resource allocations decided accordingly.

EU-GRASP places special emphasis in the role of the EU in a multi-polar world. The EU must adapt to changing global multilateralism. The EU must be steady in its promotion of multilateralism as an ideal, but extremely flexible in its multilateral practice, and find ways – for which EU governance seems particularly well fitted compared to the traditional diplomacies – to engage with legitimate sub-national, multinational and transnational non-state actors and their networks. At the same time, it must find innovative ways to address the problems of absent, competing, obsolete or ineffective multilateral structures that exist both at the regional and global level. The EU institutions must be flexible enough to work with other institutional structures or simply to create alliances with groups of countries that are promoting multilateral solutions in their regions and on the global scale, such as those of Latin America and of Africa. The "sui generis" character of the EU is strength in global multilateralism, and should not be abandoned lightly. The EU must expend more effort using the combined capabilities of the EU institutions and of EU national diplomacies to convince third parties, and less time negotiating amongst EU member states. The EU is more successful in global multilateralism when it has a unified voice; the best way of ensuring this simple voice is often, but not always, to occupy a single, EU chair. At the same time coherence is a crucial value for success in the mid- to long term, and the best way to ensure it is to apply uniformly the principles and values of the EU.

In its recommendations, the NATO study (Security Jam 2012) focuses, among others, on security issues of global concern, managing relations with emerging powers as well as on the EU defence research:

- A maritime domain policy for NATO - NATO should formalize a maritime domain policy that anticipates ships operating beyond the Euro-Atlantic area more regularly, to map out member state programmes and to push for new common platforms.

- A NATO-China Council - In light of China's increasing global influence and clear military build-up, NATO should establish a NATO-China Council (NCC) to mirror the alliance's engagement within the NATO-Russia Council. Such a platform would help establish stronger diplomatic and personal connections with Chinese counterparts both within the Alliance and at national level.

- Update of EU's Defence Industrial Policy - The EU's Defence Industrial Policy should be updated, with a focus on pooling R&D, restricting sensitive exports and developing a new generation of military equipment.

- A 'Smart Defence Mindset' for NATO - NATO should launch a programme dedicated to fostering a 'Smart Defence Mindset' amongst military personnel, national politicians and other stakeholders.

Suggestions for future research usually concern future work on specific topics as well as on methodological issues. SANDERA produced a long list of suggestions for further research. One suggestion regards the analysis of the portfolio of policy instruments at the EU-level and European level in view of defining the potential that supra-national and inter-national portfolio offers in Europe in terms of strengthening a European synergy in defence-research related items. The relationship between "vertical" integration (between Member States and the EU level within a single policy domain) and "horizontal" integration (between defence research and the ERA) should also be examined. This involves, above all, a sound understanding of the dynamics that would drive a defence community to emerge and how this would translate into demands for and taking advantage of integration instruments in ERA. New modes of research, innovation and production in the defence sector should also be analysed. Further, it would be very relevant to study the way in which the current thrust towards 'open innovation' in Europe could have an influence on the way in which public and private actors in Europe conduct research in the security and defence-related sectors.

Another issue addressed in SANDERA is the need for public and private actors to more closely cooperate on security and defence missions. Further research is required to devise ways in which such cooperation could develop. Another area of interest for future research concerns the effects of ICT on our security and the way we can defend our society. An increased interconnectedness of people, networks and increasingly machines will alter our daily practices. It will also lead to new vulnerabilities at personal level (e.g. privacy) and systemic level (e.g. a digitalised electricity grid). Research in this area will need to address a broad range of issues from the development of concepts and a vocabulary to discuss the problems and challenges, over legal norms about what presents a deliberate attack, what is a crime or an unintended consequence, political agreements on how to respond without risking an escalation of hostilities that could well spill over from the virtual to the "real" world, and regulations on liability and compensation to technological mechanisms for containment, protection and defence.

Foresight methods would be useful tools for the defence establishment. Research work would be required to adapt it to the specific needs of defence planners. While military planning is good in identifying, activating and employing expert knowledge, it could benefit from the more

inclusive and participatory character of foresight techniques. This would not only allow tapping into knowledge outside domains which are known to be relevant but also to foster ties between the defence and civilian research communities. (SANDERA)

Additional research is also required to better understand which industrial technologies, material resources and what types of skills are necessary for the EU's strategic independence. Strategic independence has a military and an economic dimension. Proactive research and a systematic screening of the relevant developments and the key technologies seem to be appropriate. Such research activity should be combined with measures in the area of science diplomacy and the monitoring of investments in strategically important sectors. It is increasingly difficult for the member states to maintain the degree of self-sufficiency they enjoyed in the past. Increased international cooperation is therefore the obvious alternative. Thus, the analysis of alternative roles that the EU could play in the procurement of defence and security and technologies becomes important. (SANDERA)

Last but not least, the relationship between defence and civilian security has encountered marked differences in views between different policy and professional communities. While it is recognised that there is a considerable convergence between the two at the technological and functional level, the institutional, legal and political divisions continue to be strong. We should explore the possibility of moving from the present fragmented concept of security to a comprehensive one that stresses the complementary and dynamics relations between its military, policing, political, economic and other components of security. The EU could take a lead in identifying and addressing the emerging dimensions of security not yet locked into the national frameworks. (SANDERA)

FORESEC repeats the importance of researching certain definitional and analytical aspects of security (i.e. on societal aspects of security, unintentional threats, external dimension of security and its link to internal security, cultural aspects of terrorism, societal resilience and cultural and social identity). In addition suggestions are made with emphasis on assessing impacts of certain challenges on security, i.e. vulnerability of societies in the EU, migration and demographic shifts and security, climate change and security, urbanisation on human security.

2.3.3 Transforming Futures

'Transforming futures' reflects the ability of FLAs to shape a range of possible futures through six major types of transformations representing the ultimate outcomes or impacts of FLA:

- Transforming *capacities and skills*
- Transforming *priorities and strategies*
- Transforming *paradigms and current visions*
- Transforming *socio-economic and STI systems*
- Transforming *behaviour, attitudes and lifestyles*
- Transforming *knowledge-based products and services*

These types of impacts need significant time after the end of the FLA to be identifiable and their identification necessitate impact assessment exercises which are beyond the scope of the EFP project. In this regard, the present section reports examples of recommendations (that would be grouped under the 'recommending futures') that may lead to transformation such as the above rather than any actual impacts.

If its recommendations are taken-up, EURACOM may transform capacities and skills as well as knowledge-based services in relation to risk assessment and contingency planning in all the energy sectors: from fuel transport, electricity generation (nuclear and fossil fuel plants), over electricity transmission, oil and gas pipelines, up to fuel storage (nuclear fuel, nuclear waste, oil, and gasification plants). EURACOM's ultimate aim is to strengthen the common understanding of threats, the establishment of common procedures and understanding of risks, developing effective and coherent tools for planning contingency measures.

EURACOM may also transform current national and European policies and strategies by proposing suggestions and options to support European policies for the protection of critical energy infrastructures. By bringing together all sectoral stakeholders (production, transmission and distribution) and the Member States authorities EURACOM may also contribute to transforming STI systems with the development of more secure, integrated frameworks, and the implementation of emergency plans, based on a holistic approach with European guidelines, new norms and standards.

SECURENV may also transform policies and strategies by supporting the development of policies, programmes and initiatives with providing advice for policy makers, programme managers and researchers dealing with security and environmental issues. SECURENV might have also contributed to transforming priorities for European research as the project defined a strategic roadmap for future security research. The SANDERA project may also contribute to transforming policies and strategies through the policy analysis toolkit that enables the assessment of policy proposal in the light of the ERA-defence research and innovation relationships.

FESTOS may contribute to transforming capacities and skills, behaviour, attitudes and lifestyles as well as knowledge-based products and services. It suggests certain measures in relation to the control of knowledge, the education of citizens, scientists and engineers, and different types of codes of conduct as possible measures to treat the problematic issue of the dark side of technology. Common to these three groups of measures is the fact that they try to approach the development of potentially dangerous knowledge on the level of the individual scientist, researcher or engineer who is involved in the development of new technologies or its applications.

FESTOS may also transform current security priorities and strategies with a set of measures aiming at structural changes in security and technology policies. One possible measure in this regard is Security Impact Analysis (SIA). SIA could be extended from the national level to cover the global, European, research and enterprise levels. Another dimension of policy measures to cope with potential emerging threats should be R&D programmes promoting responsible research which increase the knowledge needed around certain possible threats. Several themes that could be possibly included in national and/or European programs include foresight and scenario methodologies; knowledge control; ethics and freedom of science; technology and research on ICT, nanotechnology and new materials; biotechnology; robotics; cognition and converging technologies.

FESTOS also contributes to transforming STI systems. It is highlighted that there is a need to involve existing institutions in the Member States and in European Union occupied with early warning in to the process. In this regard the project examines two types of institutes: an

imaginary Committee for Threat Assessment and another institute to be created based on the already existing Situation Centres that occur on local, national and regional level.

3 Conclusions

The security FLAs mapped represent a set of forward-looking activities with a European, if not international, scope. The issue of cooperation to transform strategies and visions in dealing with the certain (grand) challenges facing societies is at the core of their justification. Overall, there is a focus on an ambition towards common activities and shared ways of doing things, which may reflect the fact that European security policy has not yet reached a degree of maturity. Engaging key stakeholders and decision shapers as well as generating shared visions and scenarios of European security are among the major rationales in an effort to reverse the fact that defence and security have been confined within national borders.

The domain coverage of the security FLAs shows the links of the security area with socio-economic issues as well as technological developments as in the area of ICT. At the same time the strong linkages to the transport area reflect the importance of security research in (critical) infrastructures and interconnected networks, indeed an area of major importance for the EU.

Not surprisingly, the major target audiences are public corporations, government departments and agencies but also the European institutions, followed by other European EU bodies and international organisations (OECD, UNESCO, UNIDO, etc.) and NGOs. The surprise here is that the corporate sector is less considered as target audience.

Having an international scope, the security FLAs mapped are rather different in their outputs than more traditional security FLAs originating in the defence sector where key technologies and technology roadmaps prevail. In this case the primary outputs refer to drivers, trends, scenarios, wild cards, and models / frameworks.

There is no clear separation between drivers, trends, and megatrends. It is often the case that what is emphasised as megatrends or trends is also implicitly or explicitly linked to grand challenges (emergence of new powers, scarcities, climate change, inequalities, demographics, migration, health, role of the individual, importance of non-state actors, financial crisis, new types of conflicts, etc.). However, they all have a strong security perspective in their analysis.

Scenarios have a particular role. They are usually reflections of future states of the world in the event of particular security threats or risks materialise. Hence, they are quite specific. However, there are also a couple of cases where more holistic scenarios are developed, and these mainly deal with the future role of the EU.

Similar to the case-specific scenarios certain wild cards are also discussed, again with the security implications at the core of their analysis. Further, the security FLAs mapped can form a rich source of analytical and conceptual models about the notion of security, security impacts and implications as well as decision support tools.

The recommendations put forward may concern specific areas of security (like marine security). However, there are several that address European security and defence policy and the need for international cooperation while they also promote the role of the EU in a multi-polar future world. Suggestions for further research form a rich source for future research

programming covering both methodological and definitional aspects of security, as well as security implications from certain (grand) challenges.

The 'transforming futures' impacts are the ultimate impacts FLAs could have. They need significant time to materialise. In this regard, the security FLAs mapped can only provide indications of possible future transformations if the recommendations they produce are implemented rather than actual impacts. It is characteristic that several FLAs may lead to transformations of all possible types. Some FLAs mainly address capacities and skills, behaviour, attitudes and lifestyles and knowledge-based products and services, while others are primarily concerned with priorities and strategies and the socio-economic and STI systems in the security area. This reflects the two main concerns in security research, i.e. the first related to skills, attitudes, knowledge and services around threats and risks, and the second being about upgrading security policies and strategies to the European level and supporting them with the necessary structures.

4 Reference and sources

Note: The references listed in this report are mainly those related to previous and ongoing mapping activities. In order to map each of the **security**-oriented forward-looking activities (FLAs) discussed in this report we have reviewed many more references and sources that are linked to individual cases in the online Mapping Environment.

Jones, B., Amanatidou, E., Popper, R., (2012) *3rd EFP Annual Mapping Report: Health Futures*, Manchester: The University of Manchester, European Foresight Platform (EFP).

Popper, R. and Teichler, T., (2011) *1st EFP Annual Mapping Report 2010-11: Practical Guide to Fully-Fledged Mapping of Forward-Looking Activities (FLAs)*, Manchester: The University of Manchester, European Foresight Platform (EFP).

Popper, R. (2011) "Wild Cards and Weak Signals Informing and Shaping Research and Innovation Policy", Paper presented at the 'Fourth International Seville Conference on Future-Oriented Technology Analysis (FTA): FTA and Grand Societal Challenges – Shaping and Driving Structural and Systemic Transformations', Seville, 12-13 May 2011.

Popper, R. (2009), *Mapping Foresight: Revealing how Europe and other world regions navigate into the future*, EFMN, Luxembourg: Publications Office of the EU, European Commission, 126pp, http://ec.europa.eu/research/social-sciences/pdf/efmn-mapping-foresight_en.pdf

Popper, R. (2008), Foresight Methodology, in Georghiou, L., Cassingena H., J., Keenan, M., Miles, I., and Popper, R., The Handbook of Technology Foresight: Concepts and Practice, Edward Elgar, Cheltenham, pp. 44–88.

FLAs mapped:

1. http://www.mappingforesight.eu/initiative/eu-grasp/
2. http://www.mappingforesight.eu/initiative/sandera/
3. http://www.mappingforesight.eu/initiative/europe-s-evolving-security-drivers-trends-and-scenarios-foresec/
4. http://www.mappingforesight.eu/initiative/foresight-of-evolving-security-threats-posed-by-emerging-technologies-festos/
5. http://www.mappingforesight.eu/initiative/security-jam-2012/
6. http://www.mappingforesight.eu/initiative/dcdc-global-strategic-trends-2040/
7. http://www.mappingforesight.eu/initiative/star-trans/
8. http://www.mappingforesight.eu/initiative/nic-global-trends-2025/
9. http://www.mappingforesight.eu/initiative/espas-global-trends-2030/
10. http://www.mappingforesight.eu/initiative/acrimas/
11. http://www.mappingforesight.eu/initiative/seron/
12. http://www.mappingforesight.eu/initiative/euracom/
13. http://www.mappingforesight.eu/initiative/securenv/
14. http://www.mappingforesight.eu/initiative/dessi/
15. http://www.mappingforesight.eu/initiative/straw/
16. http://www.mappingforesight.eu/initiative/pats-privacy-awareness-through-security-organsiation-branding/