Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Content   *I&S*

The Way Ahead

I&S Monitor

REFERENCING THE FUTURE: THE EU'S PROJECTED SECURITY ROLES AND THEIR R&D IMPLICATIONS

Brooks TIGNER

Abstract: This paper describes the methodology of how the FOCUS project's initial 24 thematic scenarios – covering five security "Big Themes" – were cross-referenced and distilled to a single Reference scenario for each of the five Themes. Each Reference scenario thus points to a future security role the EU could be expected to play in the year 2035 and its implied Security Research objectives needed to support that role – all thus forming the basis for FOCUS' ultimate goal: a roadmap for future EU Security Research.

Keywords: EU security, EU security research, R&D, reference scenarios, foresight, Petersberg, critical infrastructure protection, cross-border resiliency, research roadmap, scenario-based planning.

Introduction

One of the culminating efforts of the FOCUS project's foresight work was to construct a final set of reference scenarios (REFs) to represent the range of possible security roles that the EU might play by the year 2035 – and to synthesize the kinds of R&D that might be needed between now and then to support those roles. This lay at the heart of FOCUS' Work Package 8.1, and was based on the solid research of prior work packages by project partners, namely the 24 thematic scenarios they produced. These scenarios were grouped into sub-sets according to the five Big Themes that guided FOCUS' research regarding potential EU security roles of the future and their R&D implications.

The 24 thematic scenarios, plus additional preparatory analysis, were the basis for WP8.1's deliverable. Its principle goals were to define a methodology for cross-referencing the 24 scenarios, extract or "filter" five REF scenarios from them—i.e., one for each of the five Big Themes—and identify transversal complementarities as indicative pointers to future decision-making for the planning of security research out

to the year 2035. FOCUS' five Big Themes of foresight research are: Future concept of comprehensive approach and EU homeland security; Natural disasters and global environmental change; Critical infrastructure and supply chain protection; EU as a global actor based on the Petersberg tasks; and EU internal framework.

The View from the Outside

An important preparatory step that preceded the REF filtering work was to gather outside expert opinion about the 24 thematic scenarios themselves. This was carried out within WP8 in September 2012 via an on-line questionnaire led by partner SFU-CEUSS. The latter's questions were structured so as to enable FOCUS to rank the 24 thematic scenarios according to the various permutations of their high-vs-low likelihood of transpiring in the future and their high-vs-low impact on Europe's security and possible EU roles. The permutations were:

- High Impact/High Probability
- Low Impact/High Probability
- High Impact/Low Probability
- Medium Impact/Medium Probability.

The application of these variables by outside experts to the 24 scenarios resulted in the identification of one high-priority "Masterplan" (high impact/high probability) scenario and a number of "Trend" scenarios (medium impact/medium probability) across the five themes.

For example, under the Comprehensive approach Big Theme the sub-set scenario known as "Security to sell" took as its main premise that market economics would be the central driver of the EU's security R&D developments. The results of the on-line questionnaire identified this as a Trend scenario, meaning it was a reasonable and fairly likely description of the future, with fairly likely implications for security R&D.

In similar fashion, the Critical Infrastructure Big Theme's sub-scenario—"Not over my border"—was also characterised as a medium-likely Trend scenario. In this particular scenario, security research shifts from isolated technology developments at national level to system integration that facilitates cross-border resiliency to threats to critical infrastructures, based on common response guidelines agreed by the EU and its 27 member states.

By contrast, the "Hands across the ocean" sub-scenario under the Big Theme of EU-as-global-actor-based-on-wider-Petersberg-tasks was clearly pinpointed as a Masterplan scenario. This sub-scenario centred around a future where multilateralised technologies are used to counter cyber threats. Many outside experts considered this to be highly probable, with major implications for the EU's future security research needs.

From the results of the questionnaire analysis was also extracted regarding the outside experts' view about the anticipated key technologies that commonly applied across each subset of scenarios. These broke down as follows:

Big Theme: Comprehensive approach

- Chemical and biological sensors; X-ray technology
- Imaging technologies
- Decision support software
- Mobile broadband communications
- Convertible technologies
- Multi-use platforms
- IT platforms
- Response capabilities

Big Theme: Natural disasters and global environmental change

- Smart power grids
- Decentralized power generators
- Robot technologies

Big Theme: Critical infrastructure and supply chain protection

- Data protection technology
- IT security technology

Big Theme: EU as a global actor based on the wider Petersberg tasks

- Unmanned aerial vehicles
- Image processing equipment
- IT intelligence

Big Theme: EU internal framework and EU homeland security

- Cyber intelligence technologies
- Space technologies

Such results informed the structuring and content of the subsequent REF scenarios in several ways. They subsequently validated the construction of two of the five final REFs scenarios—*"Security as Societal Science"* and *"No Land is an Island"*—as extreme scenarios. They also supported the construction of the reference scenario, *"Borderless Threats = Mission Creep,"* and its emphasis on generalized security research. The results also supported the construction of the REF scenario *"Policy Drives All in a Have/Have-Not World"*—reflecting its possible trend toward its more extreme descriptors—and, finally, they confirmed the inclusion of the notion of multilateralized technologies, particularly in the information and communication sector, across all the REF scenarios.

Generating the REF Scenarios

The next step was then to derive one single reference scenario (REF) from the five sub-sets of Big Theme related scenarios. While scenario derivation generally lends itself to any number of methodologies, the two most logical approaches deemed suitable in this case were either (a) choosing one from each of the sub-sets to represent

the entire set, or (b) fusing the most appropriate descriptor elements from each to produce a representative composite scenario. Given the large diversity of sub-scenarios within each Big Theme, the former approach—i.e., choosing one sub-scenario only to represent its entire Big Theme—was rejected for its risk of omitting relevant descriptors in its sister scenarios, or for biasing the Big Theme towards one particular extreme projection or the other. The composite-scenario approach was chosen instead. The challenge then became one of devising a methodology to produce composite REF scenarios for each of the Big Theme scenario sub-sets.

The methodology was derived from SecEUR's extensive EU policy knowledge, its analysis and previous research work into current and future trends for policy within European Institutions and international organisations, and its knowledge of forthcoming institutional developments that directly concern the five Big Themes. SecEUR's approach was centered on the creation of a standard "scenario generator" for each Big Theme's sub-set of scenarios, with each generator listing the basic descriptive elements of all those scenarios. Each descriptor was then mapped against multiple relevant EU policies (EP reports, COM directives and communications, Council declarations), external documents such as ESRIF[1] (for whose R&D forecasting work several members of the WP8.1 team were involved) and the political stances of the 27 Member States (via Council positions). The result was to "filter" or assess whether the descriptive element remained valid for the 2035 timeframe, as projected through the assumptions that underpin those policies.[2] The entire generator analysis was cast into tabular form for each scenario within each Big Theme's sub-set of scenarios.

A given descriptor element was accepted or rejected whether it received more "likely" or "unlikely" assessments as compared against the reference documents or policy stances. Those descriptor elements which received the same number of likely *vs* unlikely assessments were categorised as "neutral" and thus carried no weight in final assessment of that descriptor element's tendency to project into the future.

For example, Big Theme Comprehensive Approach's scenario 3 entitled, "'EUCIP' – Research system for European critical infrastructure protection" obtained the following essential descriptor: "Security Research: training for different missions, based on established practical and academic curricula." This descriptor was compared against its relevant reference documents/stances to determine its likelihood of projecting to the future (see Table 1).

This comparative mapping/filtering exercise was carried out across all 24 thematic scenarios. The remaining or "surviving" descriptor elements were then regrouped accorded to their relevant Big Theme, and reconstituted textually into a new reference (REF) scenario as representing the most probable projection of that Big Theme to 2035.

**Table 1: Comprehensive Approach- Scenario 3:
Research for European critical infrastructure protection.**

Basic scenario/ research descriptor	Modulating filter	Likely evolution or projection of scenario / research element	Final combined result of filter element impact
Technology main guarantor of critical infrastructure protection	*From Commission:*		
	1) Commission staff working paper *A Budget for Europe 2020: the current system of funding, the challenges ahead*, SEC(2011) 868 final	1) Likely	
	2) As shown by numerous projects assessing the public perception of security technology (e.g. SurPRISE, RESPECT, IRISS, INDECT, SUBITO, CAPER, BAYSILIS, SAPIENT, SMART, DETECTER), technology-driven Security Research alone is highly unlikely to benefit of general public support in future.	2) Unlikely	
	From European Parliament:	3) Neutral:	
	3) Plenary resolution of 12.06.2012 on Critical Information Infrastructure Protection (CIIP)	EP calls for strong technology standards AND strong EU policy oversight	
	From EU Council:	4) Unlikely	
	4) EU Action Plan on Combating Terrorism, 09.12.2011		Final tally: *UNLIKELY*

The resulting new REF scenarios depicted alternative futures for security research in 2035 which support the EU's projected exogenous security roles (i.e., its responsibilities that derive from threats and challenges beyond the EU but which must be dealt with internally since they would directly impact the security of its citizens).

Additional Validation

The new REFs were subsequently resubmitted to their respective work groups within WP8 for further refinement and validation. WP8.1 partners were also tasked to list the main security research stakeholders that logically flow from each of the REFs and

to identify their derived threats, technologies, research needs and especially the ethical dimensions these imply.[3] Each standardized REF scenario package developed by WP8.1 thus comprises its textual version, its main descriptors in bulleted form, major Security Research stakeholders and a table listing the REF's implied threats, technologies, research needs and ethical aspects.

The final broad task was to analyze the REFs as the first step toward construction of the FOCUS roadmap process. This analysis was three-fold. First, the five REFs were compared against each other to identify:

- transversal external threats and related impact on the security of EU citizens
- translation mechanisms these represent between external threats and their impact
- impact of exogenous challenges on the Member States and the limits to coherent EU roles to isolate the gaps in security research norms, standards and procedures.

Second, WP8.1 partners assessed the differential impact of the 2035 REFs at national level to determine their relevance across various EU Member States. This yielded some interesting findings such as how the REFs ranked according to their impact at national level or, conversely, how the countries were ranked according to the impact which the REF scenarios had on them.[4]

Finally, FOCUS partners helped refine the requirements for the 2035 timeline by comparing the R&D outcomes of other relevant FP7 projects against the five REF scenarios to derive recommendations for FOCUS' roadmap requirements. Indeed, the results of key auxiliary analysis were integrated into the REFs and their transversal analysis in order to enrich their relevance and utility for guiding future Security Research choices.

In the end, these multiple work strands converged to produce a set of Reference Scenario results that will populate the final work of WP8—and the FOCUS project itself—in the form of an EU Security Research planning roadmap for the 2035 time frame.

Notes:

1   European Security Research & Innovation Forum, *ESRIF Final Report* (December 2009), http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

2   A compendium of all EU policy documents relevant to the constituent elements of the FOCUS' 24 thematic scenarios for purposes of generating the REFs was compiled and organised by WP8.1 team leader SecEUR in the months leading up to the final REF scenarios' creation. The compendium was drawn mainly, but not exclusively, from the previous three years (early 2009 to mid-2012), on the assumption that any earlier documents would be too contextually distant from the EU's Lisbon Treaty. The compendium's policy documents were then correlated with the relevant descriptors of each of the 24 thematic scenarios. For example, the 05 June 2012 draft report by MEP Indrek Tarand—regarding climate-driven crises and natural disasters—called on the EU to place climate change and its ramifications for security and defence "at the core of analysis" of risks concerning future crises and conflicts. This and related policy stances across the EU institutions were directly applied to the descriptors of several of FOCUS' Big Theme scenarios (notably those related to the "EU as a global actor based on the wider Petersberg tasks" and the Big Theme, "Natural disasters and global environmental change"), thus confirming the scenarios' assumptions about future research needs linked to potential conflicts posed by climate change to the EU.

3   The ethical implications of the technology/R&D needs implied by each REF scenario were derived from a comparison against the recommendations of the EU-funded project known as PRISE ("Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies"). The latter was among the first batch of civil-security oriented "test case" projects funded by the EU during 2003-2006, which paved the way for the EU's larger EUR 1.4 billion Security Research programme of 2007-2013. For details about PRISE, see www.prise.oeaw.ac.at.

4   See *Thematic scenario portfolio (Work Packages 3-7) with reference scenarios for "Security Research 2035,"* FOCUS Deliverable 8.1 (October 2012), pp. 124-130, available at www.focusproject.eu/documents/14976/78b744e5-9daa-432b-be3b-92316416aa65.

BROOKS TIGNER is head of technical studies at SecEUR sprl and chief policy analyst for *SECurity EURope*, the company's monthly civil security publication. He has analysed European security, defence and technology issues from Brussels for more than two decades. His longstanding analysis of Europe's homeland security capability goals affords him a singular perspective on dual-use technology trends and their application for civil security, humanitarian and crisis-management purposes. He speaks English and French and has dual Belgian-US nationality. *E-mail*: bt@seceur.info