INFORMATION & SECURITY
An International Journal

Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Procon Ltd.

Volume 29, 2013

Content *I&S*

The Way Ahead

I&S Monitor

Information & Security: An International Journal

Benesch, Goellner, Peer, Hoechtl & Seboeck, vol.29, 2013, 111-119

http://dx.doi.org/10.11610/isij.2908

SCENARIO SPACE FOR ALTERNATIVE FUTURES OF SECURITY RESEARCH

Thomas BENESCH, Johannes GOELLNER, Andreas PEER, Johann HOECHTL and Walter SEBOECK

Abstract: FOCUS ("Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles") aims namely to define the most plausible threat scenarios that affect the "borderline" between the EU's external and internal dimensions to security. This article presents scenarios about alternative futures of security research to support a comprehensive approach of the "EU 2035" as a civil security provider. Three scenarios were selected as context scenarios for alternative futures of security research afterwards they have been lined up with drivers identified in a matrix procedure. From these three context scenarios six alternative futures for security research were evaluated using the portfolio-cluster-method. The weighting was done from a dual and interdependent perspective: a) nation/ member state vs. EU-level/international approach to civil security and b) position of the scenario on the continuum of internal/external security. Finally, the article introduces each scenario for alternative future of security research in detail.

Keywords: Comprehensive Approach, Scenario Space, FOCUS, Security Research 2035, Generalised Security Research System, Nationalisation of Security Research, European Critical Infrastructure Protection, EUCIP, Incident Management, Security Economics, Public Health Research

Introduction

FOCUS ("*Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles*") aims wide but with concrete policy guidance in mind: namely to define the most plausible threat scenarios that affect the "borderline" between the EU's external and internal dimensions to security – and to derive guidance for the Union's future possible security roles and decisions to plan research in support of those roles. FOCUS brings together 13 partners from 8 countries, including universities, industry, think tanks and security information providers.

Reflecting the cross-border and cross-sector nature of current security threats and challenges as well as the complexity of instruments and objectives in security policy along the internal-external continuum, the comprehensive approach focuses on the holistic nature and broad trade-offs involving societal goals in order to increase the security of the EU and its citizenry as a whole. It aims to find and implement overarching solutions to problems, with broad effects and based on complementarity of actors, while considering all available options and capabilities, as well as the normative end-state of the security of society as a whole. A comprehensive approach also entails the tackling of cross-cutting issues in home affairs.

In this article we present six future scenarios for "security research 2035" and explain the generation through a matrix. Afterwards the six future scenarios are put in a scenario space with the two independent dimensions: national/member state vs. EU-level/international approach and internal-external security continuum.

Development of future scenarios for "security research 2035"

This article presents scenarios about alternative futures of security research to support a comprehensive approach of the "EU 2035" as a civil security provider. A list of cross-cutting or "transversal" aspects, which all of the developed six scenarios for "security research 2035" have generally in common, were identified.[1] Those transversal aspects relate to future fields of action and needed expertise in most of the six future scenarios for "security research 2035," including identification of tools and systems for comprehensive crisis management to overcome present and anticipated future weaknesses.

In relation to a report on alternative future models of comprehensiveness developed scenarios from FOCUS foresight processes include conceptual analysis and scholarly work as well as empirical work. Empirical work was based on quantitative conceptual analysis, expert questionnaires, and guided interviews. The level of analysis addressed were context scenarios (future concepts of the comprehensive approach as main reference for exogenous EU roles).

From these scenarios, three were selected, based on results of internal project workshops and in accordance with their relevance to tangible future security research themes in the 2035 time frame of the project. Scenario selection also followed the principle of integration of expert and policy scenarios.

The scenarios for alternative futures of security research in support of the *"Comprehensive approach 2035"* were developed with the use of the matrix shown in Table 1. This matrix provides a structure for the qualitative description of the combination of thematic tracks as drivers and context scenarios.

Table 1: Matrix for qualitative description of the combination of thematic tracks (as drivers) and context scenarios

Drivers identified	Context scenarios		
	Policy strategies consenus scenario	Policy strategy leftovers scenario	Materialism scenario
EU cohesion, decision-making and, more generally, governance	1	16	31
Regional / international / global distribution wealth	2	17	32
Climate change	3	18	33
Crisies resulting from scarcity of resources	4	19	34
Debendency on Supply chains and reliability on the stability of resource sources (stability of providing countries)	5	20	35
Dependandy on information and communication technology, and technology in general (adress cascading breakdown of systems)	6	21	36
Willingness to invest in preparedness	7	22	37
New methodologies for collecting and integration data from various different sources	8	23	38
Intelligent, knowledge-based focusing and filtering functions for new social media nad other open information source monitoring	9	24	39
Integrated situational pictures as facilitation for networked operation command structures	10	25	40
Information exchange among civilian and military actors in orders to provide common, timely and relevant situational awareness	11	26	41
Decision-making tools based on joined-up situation analyses, including their use to secure public acceptance and support	12	27	42
Standardized skills development and integrated information systems for a effective coordination of resources as well as to cooperation between EU Member States	13	28	43
Training schemes for technology use, including new social network technologies	14	29	44
Advancement and integration of approaches to foresight, with special consideration of the following	15	30	45

During two internal team workshops of the FOCUS consortium, the context scenarios were analysed, assessed critically and weighted by FOCUS subject matter experts. The weighting was done according to a dual and interdependent perspective (two dimensions):

- nation/member state vs. EU-level/international approach to civil security and security research;
- position of the scenario on the continuum of internal/external security.

As a result, three scenarios were selected as context scenarios for alternative futures of security research. These three selected context scenarios were lined up with drivers identified in a matrix procedure. This was done based on interviews with internal as well as external experts. The resulting matrix was then compiled via question and feedback loops within the FOCUS consortium.

Six alternative futures of security research in support of an "EU comprehensive approach 2035" were derived from the resulting matrix in Table 1. The combination of cells led to key categories through the use of cluster methods. These methods were then combined with a portfolio-analysis and the resulting characteristics are explained in the next section.

Characteristics of the Identified Security Systems

Based on the two dimensions and their uptake in this article, the six alternative futures for security research in support of an "EU comprehensive approach 2035" can be located in the scenario space shown in Figure 1.

The generalized security research system is located on the internal and external security continuum, but definitely closer to an EU-level/international approach. The nationalization of security research is placed in the internal security and shows a national/member state approach. The EUCIP research system[2] points out internal security in a high EU-level/international approach. The security incident management research is clearly located in the internal security continuum and reaches the border between national and international approach. The security economics research system

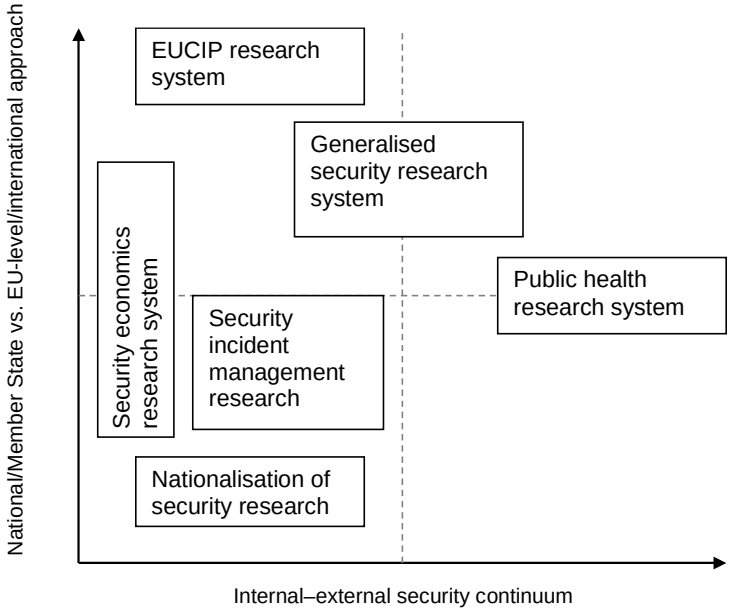

Figure 1: Scenario space for alternative futures of security research in support of an "EU comprehensive approach 2035".

is at the internal security and builds the connection between the nationalization of security research and the EUCIP research system. The public health research system is the only scenario that lies fully within the external security continuum and can be a national as well as an international approach.

The identified six scenarios, which are contextualised in the scenario space explained above, will be introduced in more detail.

Generalised security research system

The EU 2035 has developed a common securitisation model on the basis of which it decides which topics fall under security research and which do not. National security research programmes were integrated on the European level. For agreed securitised issues, requirement profiles for politically agreed EU roles as a comprehensive security provider are stipulated. The identified gaps are then addressed by research. Research results form the basis for the design of further capability development, skill development and training programmes for different types of strategic and operational missions (socio-economical, environmental, societal and political missions), covering the full crisis management cycle (from prevention to reconstruction/recovery). Those programmes also have led to the definition of systematic qualification profiles in terms of human resources, structural and technical advances. They have been as well embedded into academic curricula and the research of security policy.[3] However, while the EU 2035 sees itself as an open system, its security research system is homeland-focused and practically based on a concept of management of integral risk in the EU territory, following an all-hazard approach. Research results are fed into a trans-disciplinary information architecture system for broad and sustainable accessibility.

Nationalisation of security research

The EU Member States 2035 consider national security, security policy and security research as a matter of sole and exclusive national responsibility. The matching concept of the security of the Union as a whole has lost practical relevance. Nevertheless, Member States consult each other on a regular basis and, where appropriate, establish common security research initiatives, with focused scope. While, consequently, the concept of comprehensiveness is not followed any more on the EU level, it has remained essential for security research as a multi-disciplinary task, including cross-national cooperation for efficient use of resources and collaboration in the anticipation and prevention of threats and risks. Apart from that, security research is planned and performed on national levels. They are based on respective national visions of how to overcome the compartmentalisation, duplication and overlapping of policies and institutional frameworks. The aim of security research 2035 in this scenario is to build a

more integrated vision of the various factors affecting security and responses to threats, in order to ensure a more coordinated and effective *comprehensive approach* on the national level.

Research system for European critical infrastructure protection (EUCIP)

Security research 2035 is a system on the EU level that focuses on supporting European critical infrastructure protection by technological innovation in order to guarantee interoperability between systems and data, including non-technological strategies to develop effective coordination of security related national bodies at the European level for managing and coordinating effective information exchange for issues like terrorism, financial and economic insecurity, cyber threats, uncontrolled migrations, emergency and civil protection, organised crime, health (early detection of epidemics), intelligence, etc. A main security research issue in the 2035 timeframe is data integration: the extent to which standardisation is used across multiple organisations or sub-units of the same organisation. Data integration provides the benefits of improved managerial information for communication, improved operational coordination across sub-units or divisions, and improved strategic planning and decision making. However, data integration can also increase costs by increasing the size and complexity of the design problem or increasing the difficulty in getting an agreement. Therefore, choosing the appropriate level of data integration may require trading off coordination against decreased local flexibility and local effectiveness. Orthogonal disciplines, combining time series analyses, visualisation methodologies, and combined network and sensitivity analysis are required to prepare highly heterogeneous data sets for further use as integrated analysis. This task requires a combined bottom-up approach, connecting academic disciplines for broad inclusive foresight involving various stakeholders from within and outside the EU.

Security incident management research [4]

Security research 2035 is conducted at the European level and address security incident management in homeland security, in disaster management, and in the European Security and Defence Policy (ESDP). Security research includes research for monitoring instruments as well as for lessons learnt which help to support critical “targets” on the EU and Member State levels, and it has overcome the security–safety divide. Security research directly contributes to resource allocation in the security sector, including budgeting and financial resources, information and communication resources, and infrastructural resources. Security research as well contributes to improving an EU-specific legal compliance framework to collectively support and protect the security/safety of EU citizens against external impacts.

Security economics research system [5]

Security research 2035 has been redesigned into a security economics research system that contributes to improving the protection of government and non-government organisations (NGOs), the citizens as well as the territory of the European Union from civil (including terrorism and organised crime, etc.), political, technical, environmental, socio-economical and legal risks/hazards, either man-made or non-man-made, either originating from within the EU or from outside. Research practice focuses on centralised and de-centralised economic and administrative systems to identify and avoid possible vulnerabilities; on technology assessment; and on supply chain networks (including banking, financial and insurance networks). Security research 2035 essentially comprises scenario development and simulation. The main aim of the research is to develop marketable products, procedures and services for EU and state agencies as well as companies and businesses within the European Union.

Public health research system [6]

Security research 2035 is based on the conviction that the health of the citizens of the European Union is the most valuable asset of the EU and its economy. This research system includes all existing and individual health care systems of the respective Member States. The main objective is to develop common standards in fields such as public health structures and processes, budgeting-infrastructure, facilities and capability development. Research in practice mainly works on mission scenarios that address biological, chemical, radiological, and nuclear threats. Moreover, research develops specific public health security and risk products, procedures and services within the scope of individual health care topics.

Conclusion

Future EU security research should contribute to the preparation of rules for processing and implementing a suitable concept leading to security of both the Member State and the Union as a whole. Future security research should also propose ways to manage specific factors, vulnerabilities, risks and possibilities to common aims, which will contribute to the security and development of the EU as a Union. As a next step the following key uncertainties have to be analysed for a further evaluation of the six scenarios:

1. EU policies with regard to third countries: Will security be considered as a key factor and mechanisms for coordination between security and other related policies developed?

2. Development and management of operational instruments including, but not confined to, civil-military interaction
3. Achievable goals and objectives in supporting non-member states
4. Prevailing crisis management strategies
5. Prevailing mission roles for the EU
6. Geopolitical setting
7. Development of structural preconditions (e.g. consensus, subsidiarity, etc.) for effective EU decision making on crisis management
8. Coordination, standardisation, or integration of decision-making, efforts, and capabilities, including international combination of capabilities/pooling
9. Development of burden-sharing and division of labour between all actors involved.

Acknowledgement. This paper reflects research within the FOCUS project, www.focusproject.eu. FOCUS is co-funded by the European Commission under grant agreement no. 261633, 7th Framework Program, theme "Security", call FP7-SEC-2010-1, work program topic 6.3-2 "Fore sighting the contribution of security research to meet the future EU roles." This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained therein.

Notes:

[1] Barry Buzan, Ole Wæver, Jaap De Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner Publications, 1998).

[2] Klaus Niemeyer, "Simulation of Critical Infrastructures," *Information & Security: An International Journal* 17 (2005): 120–143, http://dx.doi.org/10.11610/isij.1708.

[3] Barry Buzan and Ole Wæver, *Regions and Powers. The Structure of International Security*, Sixth edition (Cambridge, UK: Cambridge University Press, 2008).

[4] Jin Ki Kim, Raj Sharman, H. Raghav Rao and S. Upadhyaya, "Efficiency of Critical Incident Management Systems: Instrument Development and Validation," *Decision Support Systems* 44 (2007): 235-250.

[5] Ross J. Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore, "Security Economics and European Policy," in *Managing Information Risk and the Economics of Security*, ed. M. Eric Johnson (New York, NY: Springer, 2009), 55-80.

[6] David Stuckler, Sanjay Basu, Marc Suhrcke, Adam Coutts, and Martin McKee, "The Public Health Effect of Economic Crises and Alternative Policy Responses in Europe: an Empirical Study," *The Lancet* 374 (2009): 315-323.

Thomas BENESCH, researcher at the Danube University Krems.
E-mail: thomas.benesch@donau-uni.ac.at

Johannes GOELLNER is Senior Researcher & Deputy Leader of the EU Research Project FOCUS and Course Director of the Master of Science (MSc) Program "Risk Management" at the Danube University Krems (Inhouse Consultant). In a further employment, he is Head of the Section Knowledge Management of the Department of Central Documentation and Information Service at the National Defence Academy of the Austrian Armed Forces, Vienna. Johannes Goellner's research areas and consulting foci include trend analysis and scenario management (theoretical and methodological approaches for large scale global developments).
E-mail: johannes.goellner@donau-uni-ac.at

Andreas PEER, researcher at the Danube University Krems.
E-mail: andreas.peer@donau-uni-ac.at

Johann HOECHTL graduated from Vienna University of Technology. His current research focus is in the topic of e-Participation, Open Data, the semantic web and Web 2.0. *E-mail*: johann.hoechtl@donau-uni-ac.at

Walter SEBOECK is Head of Department for Management and Economics and the Center for Infrastructural Security at Danube University Krems. His research background is in e-policy making and e-Government reform.
E-mail: walter.seboeck@donau-uni-ac.at