INFORMATION & SECURITY
An International Journal

Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Procon Ltd.

Volume 29, 2013

Content *I&S*

Volume 29, Number 1

Volume 29, Number 2

Scenarios and Security Research Planning

The Way Ahead

I&S Monitor

Information & Security: An International Journal

Tagarev & Ivanova, vol.29, 2013, 21-33 http://dx.doi.org/10.11610/isij.2902

ANALYTICAL SUPPORT TO FORESIGHTING EU ROLES AS A GLOBAL SECURITY ACTOR

Todor TAGAREV and Petya IVANOVA

Abstract: Making decisions on major investments, including investments in security research, requires good grasp of the future, which by definition is uncertain. This paper presents the analytical process, methods, and tools, including the DSTO Scenario Analysis Tool Suite, used in the elaboration and selection of a set of context scenarios and possible new roles for EU as a global actor based on the wider Petersberg tasks. Results of this exploratory process within the FP7 FOCUS project are intended to derive suggestions for the EU's security research planning. The conclusion emphasises the critical importance of providing rigorous analytical support, in particular when security foresight involves subject matter experts that are not part of a dedicated research team.

Keywords: Security foresight, uncertainty, scenario design, alternative future, context scenario, participatory foresight.

Introduction

Making decisions about the future always involves uncertainty. The level of uncertainty is particularly high when policy makers and planners try to predict the features of the future security environment and to derive requirements, e.g. where to focus security research efforts.

In approaching uncertainty, Paul Davis of Rand Corporation distinguishes between *normal* and *deep* uncertainty, where 'normal' applies to situations where one understands the phenomenon at hand and how to value outcomes, and can apply standard versions of sensitivity or probabilistic analysis. Davis defines *deep uncertainty* as the condition where one does "not know with confidence (1) the model by which to describe the phenomenon of interest, (2) the relevant probability distributions, or (3) how to value the outcomes."[1]

Capability-based planning—the state-of-the art approach in defence policy making and planning, finding wider application in other security fields [2]—relies on a set of planning scenarios, or *planning situations*, to represent uncertainty. These planning

scenarios, however, are commonly designed with a particular vision of the future world in mind. As a consequence, the method is not directly applicable in reflecting possible deeper changes in the capability development environment. Such deeper changes may be a result of the emergence of new threats, geostrategic shifts, shifts in the political and/or societal agendas, significant change in the economic environment, the emergence of a new technology with a disruptive impact, etc. In combination, such changes may lead to rather different environment, or an *alternative future*, in which one may foresee new planning situations, or scenarios.[3]

Hence, in particular, in attempts to take a long-term view such as in the FOCUS project, it is necessary to explore the space of *alternative futures* and select a number of *context scenarios*, describing alternative futures that are both plausible and distinct. Then, for each context scenario, one can explore the possible planning scenarios and use them to define requirements of interest, e.g. security research requirements.

The FOCUS project follows this logic in the exploration of the five 'big themes.'[4] For each theme, the responsible researchers first scope the problem space. At the second step they elaborate respective context scenarios and theme-relevant roles for the European Union. In the third step they define security research scenarios. In this process, the identification of plausible and challenging alternative futures may in turn lead to EU decisions to adopt one or another role as a global security actor, thus widening the Petersberg tasks as currently defined in the Lisbon Treaty. The adoption of new roles, in turn, would lead to new capability requirements—with the respective organizational, procedural, and technological aspects—and, possibly, to new requirements for security research.

This paper presents the analytical approach, tools used, and main results in the second step for the big theme "EU as a global actor based on the wider Petersberg tasks." It is structured in two main sections. The first one presents the elaboration of context scenarios for "EU as a global actor," and the second – the exploration of possible EU roles in the 2035 timeframe.

Defining Context Scenarios

In the exploration of the problem space the research team identified principal dimensions for describing EU roles as a global security player, external threats and challenges, trends, drivers and potential strategic shocks.[5] These findings were used for extrapolation of current trends and exploration of alternative paths that may lead with time to alternative future worlds. Figure 1 illustrates this approach.[6]

A simplified presentation of the process of developing context scenarios is represented in Figure 2.[7] The first two steps in this analytical process are known as *morphological analysis*.[8] In the first step, analysts define factors to be used in the descrip-

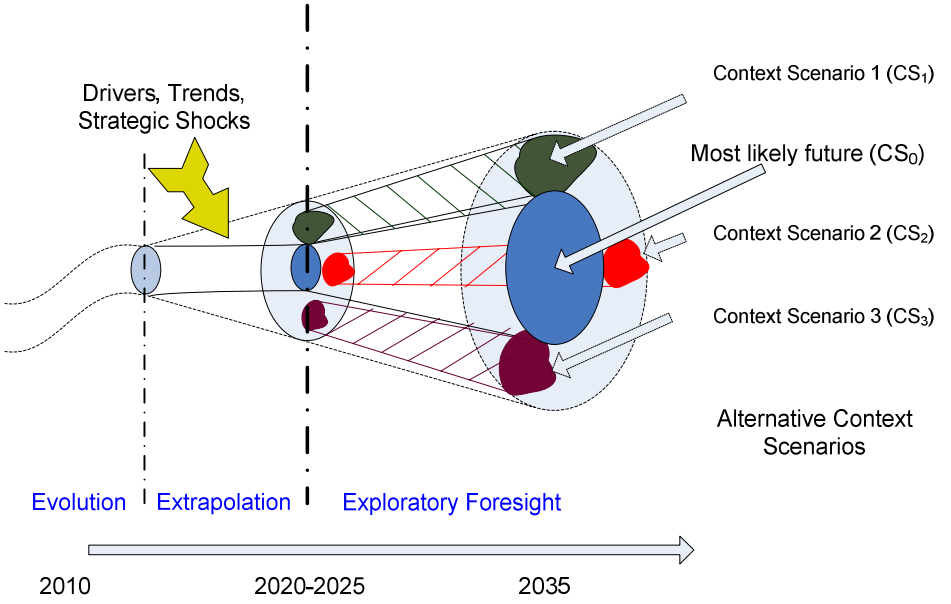

Figure 1: Illustration of the scenario foresight method.

tion of the future context. In the second step, they define states in which each factor might be in the future. Factors and states defined in these two steps need to cover exhaustively the problem space, as elaborated in FOCUS Deliverable 6.1. In addition, the possible states for each of the factors need to be mutually exclusive.

For each factor, in the third step, experts assess the probability that in the future it will be in a certain state. Given the requirement that states have to be mutually exclusive and exhaustive, the sum of probability assessments will be equal to 1.

In the fourth step, experts assess the compatibility of each pair of states for each two factors, using a scale from 1 to 5. Experts do not try to identify causal relationships; instead, they rate compatibility, with 5 indicating a very high likelihood that the two states can occur together, and 1 indicating that they are not compatible.[9]

These assessments are then used to identify among the hundreds or thousands candidate scenario configurations those that are plausible and representative. To meet the first criterion, the combined compatibility rating of all pairs in a candidate scenario configuration has to exceed a certain threshold and/or a ceiling is imposed on the number of '2's in a configuration (a configuration with one or more '1' is automatically discarded, since it contains at least one pair of incompatible states.). It is guaranteed in this way that configurations that are not internally consistent are filtered out. Secondly, the joint probability for the states in a configuration also needs to exceed a certain threshold, i.e. configurations that are internally consistent but of very low

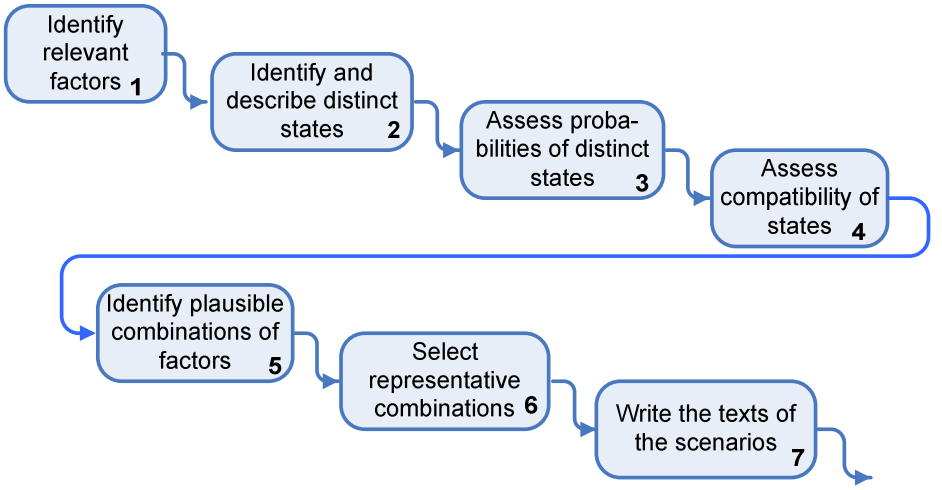

Figure 2: Context scenario development process.

probability are not included in the follow-on exploratory process. Figure 3 provides an example for the respective expert assessments.

Clustering and integer linear programming are then used to find representative configurations among those that are internally consistent and of significant probability. The first technique allows visualization of how configurations group in the scenario space. Then experts decide how many clusters to consider and select one configuration to represent each grouping, or cluster.

The second technique is used to span the scenario space, that is, to guarantee that the exploratory process will bring forth distinct capability requirements and, consequently, security research requirements.

In practice, the implementation of steps 4 and 5 cannot be efficient without adequate IT support that automates the computation of capability ratings, joint probabilities, clustering, and the resolution of the integer linear programming problem. FOCUS partner CSDM used the DSTO Scenario Analysis Tool Suite [10] for this purpose. The tool also facilitates shortlisting candidate scenario configurations.

The sixth step is finalized through expert assessments and selection of a small number of plausible configurations. At this point—and based on expert judgement—it is possible to consider interim configurations, i.e. to create configurations that combine some features of two or more of the original states for each factor. In the seventh step, analysts write the text of the context scenarios corresponding to the selected configurations.

		A Global context				B Globalisation & growth			C Security environment			D Societal Demographics &			E EU Modalities				
		1	2	3	4	1	2	3	1	2	3	1	2	3	1	2	3	4	Marginal probability
A	1	0.25	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	2	1	0.45	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	check sum
	3	1	1	0.20	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	4	1	1	1	0.10	--	--	--	--	--	--	--	--	--	--	--	--	--	1.00
B	1	4	3	2	1	0.15	--	--	--	--	--	--	--	--	--	--	--	--	
	2	3	3	5	1	1	0.60	--	--	--	--	--	--	--	--	--	--	--	
	3	2	2	4	4	1	1	0.25	--	--	--	--	--	--	--	--	--	--	1.00
C	1	1	5	1	1	5	3	1	0.25	--	--	--	--	--	--	--	--	--	
	2	1	4	3	1	5	2	1	1	0.60	--	--	--	--	--	--	--	--	
	3	5	2	4	4	1	3	4	1	1	0.15	--	--	--	--	--	--	--	1.00
D	1	2	4	2	1	5	3	1	5	3	1	0.20	--	--	--	--	--	--	
	2	4	2	2	1	2	4	5	2	2	3	1	0.70	--	--	--	--	--	
	3	4	1	2	5	1	3	5	1	2	5	1	1	0.10	--	--	--	--	1.00
E	1	2	5	3	2	4	3	1	5	4	2	4	2	1	0.40	--	--	--	
	2	2	3	4	4	3	3	4	2	3	4	2	4	3	1	0.30	--	--	
	3	3	2	4	2	1	5	4	1	2	5	4	4	5	1	1	0.20	--	
	4	5	3	5	5	1	3	5	1	2	5	1	4	5	1	1	1	0.10	1.00

Figure 3: An example for assessment of probability and compatibility.

In practice, there is an inherent tension between the need for precision and detail, and the amount of information experts may process and the time they can dedicate to understand the problem and express their expert opinion. If we account for M factors and N_x is the number of states considered for factor X, the overall number of states is:

$$N_s = N_A + N_B + N_C + \ldots + N_M$$

The number of possible scenario configurations is equal to:

$$N_A * N_B * \ldots * N_M ,$$

while the number of pairs of states, the compatibility of which has to be assessed, is proportional to N_s^2.

Therefore, for level of complexity suitable for participatory foresight,[11] i.e. involving experts that are not part of a dedicated research team, it is recommended to use no more than six or seven factors, with three to seven states for each factor. The increase in the number of factors and/or states quickly increases the time and effort experts need to invest in order to provide professional assessments.

A number of iterations were performed to refine the decision space, as follows:

- A few researchers from the project team (three in this case) worked individually in assessing probabilities and compatibility
- Individual assessments were compared to identify significant discrepancies (assessments of compatibility with a dispersion of 6 or more)

- Discrepancies were explained (e.g. unclear or misleading label or description of a state, widely differing assumptions of participating individuals, technical errors, etc.)
- Labels and description of factors and states were improved
- Other researchers conducted a new assessment, followed by comparison to check whether reasons for significant discrepancies have been eliminated.

After several iterations, researches on the FOCUS team defined the following main factors, or 'dimensions,' for presenting alternative futures for the EU as a global security actor: global context; globalisation and economic growth; security environment; societal demographics & migration; EU modalities. These five factors and the distinct states considered for each one of them are given in Table 1.

After preparing the ground for participatory foresight, further analytical steps were performed by 26 outside experts, working in four groups. For that purpose, two days of a four day exercise with upper mid-level civilians and military officers (Lieutenant Colonel level), conducted in April 2012 in the "G.S. Rakovski" Defence Academy in Sofia, were dedicated to exploring the space of contexts and future roles of the EU as a global security actor. Each group assessed probabilities for states in each factor and compatibility of pairs of states. On that basis each group received a list of configura-

Table 1. Key factors and states in the elaboration of theme-specific context scenarios.

A. Global context	B. Globalisation and economic growth	C. Security environment	D. Societal Demographics & Migration	E. EU Modalities
A1 Dominant global competitions	B1 Accelerated globalisation and growth	C1 Global collective security architecture	D1 Balanced demographics and limited migration	E1 Continuation
A2 Global management	B2 Cyclic globalisation and growth	C2 Cooperative security	D2 Expanding demographic gaps and controlled migration	E2 Differentiation
A3 Dominant regional dynamics	B3 Retarded globalisation and growth	C3 Fragmented security	D3 Migration tsunami	E3 Enhanced selective governance
A4 Conflict-dominated global context				E4 Outside EU's institutional framework

tions with higher compatibility and probability of occurrence. Figure 4 provides an example of such list.

These subsets of configurations were further subjected to cluster analysis and integer programming. Figure 5 provides an example of results of clustering.

Table 2 summarises the results of each of the four working groups participating in the scenario exercise, listing identified candidate scenario configurations. Averaged compatibility assessments by FOCUS researchers were also used in step 5 of the exploratory process to shortlist scenario configurations. Based on these results, the FOCUS team analysed again the scenario space and selected the following three distinct and plausible configurations:

- $A_2B_{1\text{-}2}C_{1\text{-}2}D_1E_1$
- $A_1B_2C_3D_3E_3$
- $A_4B_3C_3D_3E_{2\text{-}3\text{-}4}$.

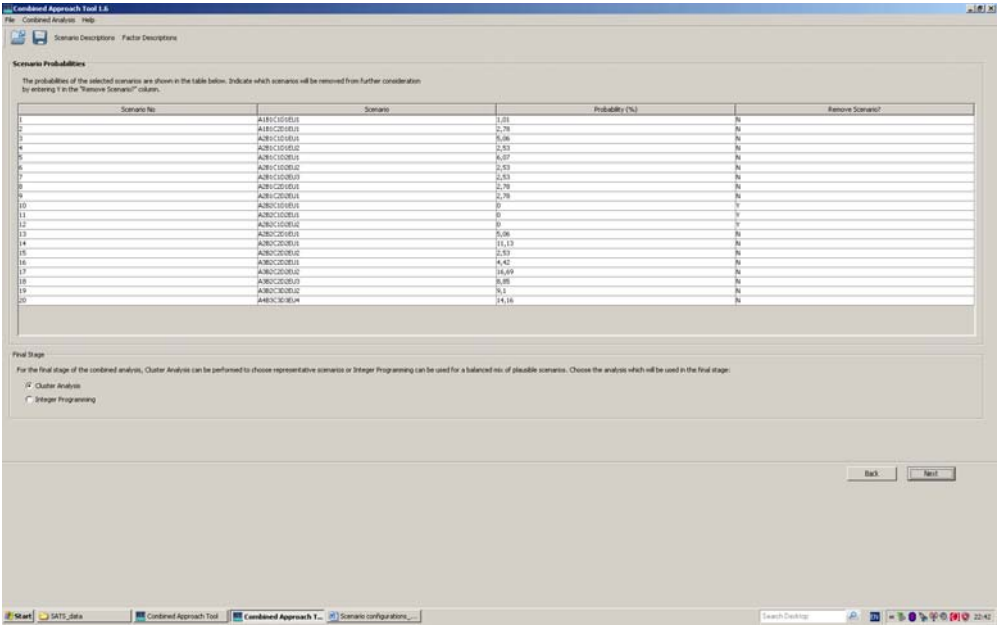

Figure 4: An example for assessment of probability and compatibility.

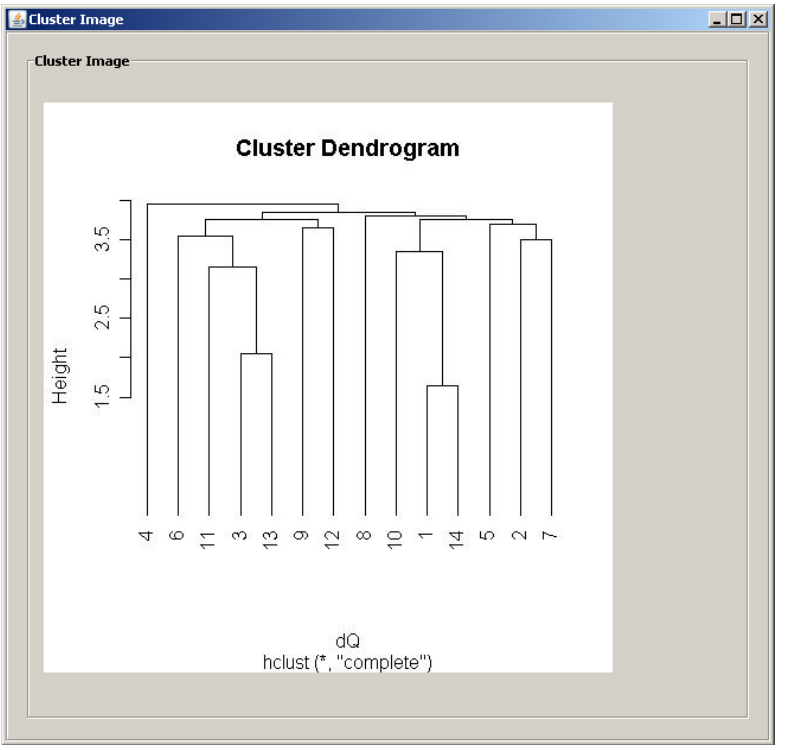

Figure 5: An example for results from clustering of candidate scenario configurations.

Table 2. Top configurations of the working groups in the scenario exercise.

WG1	WG2	WG3	WG4
$A_1B_3C_3D_2E_3$	$A_2B_1C_1D_2E_1$	$A_2B_{2\text{-}3}C_{2\text{-}3}D_2E_3$	$A_2B_1C_{1\text{-}2}D_{1\text{-}2}E_2$
$A_2B_1C_1D_1E_1$	$A_2B_2C_2D_2E_1$	$A_2B_2C_1D_2E_1$	$A_3B_1C_2D_{1\text{-}2}E_2$
$A_2B_1C_1D_2E_2$	$A_3B_2C_2D_2E_2$	$A_4B_3C_3D_3E_2$	$A_2B_3C_3D_3E_2$
$A_4B_3C_3D_2E_4$	$A_4B_3C_3D_3E_4$		

These three alternative futures were labeled respectively:

- Constructive World
- Fragmented World
- Confusing World.

At step 7 of the scenario development process researchers from FOCUS partner CSDM described in detail each of the three context scenarios.[12]

At a later stage, these results were rigorously compared with the results of other relevant security foresight studies, in particular the most recent reports of the US National Intelligence Council [13] and the Atlantic Council.[14] Based on this comparison, Uwe Nerlich from the Centre for European Security Strategies concluded that the three studies implemented similar approaches to security foresight, while their results—being specific for the goals of each study—are complementary.[15]

Foresighting EU Roles as a Global Security Actor

A similar analytical approach was used to identify plausible roles of the EU as a global security actor in the 2035 timeframe, performing 'wider' Petersberg tasks. It requires identification of *dimensions* and distinct possible *values* along each dimension.[16] Researchers on the FOCUS team developed a framework for describing EU roles with five dimensions:

(a) 'Strategy'
(b) External ambitions
(c) EU mission roles
(d) Domain
(e) Instruments in comprehensiveness of EU power.

The main difference in comparison to the framework for exploring the scenario space is that the distinct values chosen along these dimensions are not necessarily mutually exclusive. This requirement is relaxed here to reflect in the exploratory process the concept of comprehensive approach to security, accounting for the multitude of players, strategy elements, and instruments potentially used in a new role. Dimensions and the distinct values are presented in Table 3.

On the second day of the scenario exercise in Sofia, each working group was tasked to come up with two new roles related to a plausible context scenario identified by the group. The results are summarized in Table 4.[17] While the potential new tasks are described by the distinct values along dimensions 'b', 'c', and 'd' (see Table 3), in view of the comprehensive approach their implementation may involve more than one element of strategy (dimension 'a') and/or instrument (dimension 'e').

These results were further analysed and amended by the FOCUS research team that refined these roles and identified in addition a possible role in the control of CBRN proliferation. It also indicated additional possibilities in the field of extended air defence, in particular against advanced UAVs, further role differentiation that requires

Table 3. Dimensions of the space for exploring 2035 Petersberg task.

(a) 'Strategy'	(b) External ambitions	(c) EU mission roles	(d) Domain	(e) Instruments in comprehensiveness of EU power
a1 Prevention	b1 Global reach	c1 Act alone	d1 Land	e1 Military forces
a2 Deterrence	b2 Regional security player	c2 Lead (share the leadership)	d2 High altitude	e2 'Gendarmerie'
a3 Protection	b3 Neighbourhood security responsibilities	c3 Take responsibility for a particular ops area, a type of capability or capability group	d3 Outer space	e3 Intelligence
a4 Defence	b4 Addressing external dimensions of internal security	c4 Provide direct support	d4 Blue water, Sea Lines Of Communication /SLOC/	e4 'Security forces'
a5 Consequence management		c5 Support the mission indirectly	d5 Deep underwater	e5 Security governance and institution building
a6 Resilience			d6 Cyberspace	e6 Financial & Economic instruments
			d7 Energy networks	e7 Public diplomacy & cultural instruments
			d8 Arctic	

enhanced dependability, roles in response to increasing demands in implementation of R2P (Responsibility to Protect) concept.[18]

Conclusion

Scenario-based foresight cannot be rigorously performed without adequate analytical support. This paper presented the process, methods and tools used in the exploration of context scenarios and roles in theme "EU as a global security actor" of the FOCUS project. This analytical support was crucial for the successful realisation of participatory foresight. The process of exploration benefited from the involvement of experts outside the dedicated research team. They raise the awareness and bring exper-

Table 4. Future new EU roles suggested by four groups of experts.

Future EU role/task	Context scenario in which it is undertaken
Area 'Cybersecurity'	
$a_6b_4c_1d_6e_{4,1}$	$A_3B_2C_{2\text{-}3}D_2E_2$
$a_2b_1c_2d_6e_{1,5,6}$	$A_2B_2C_1D_2E_1$
Area 'Protection of Sea Lines of Communication SLOC'	
$a_3b_2c_1d_4e_4$	$A_3B_2C_{2\text{-}3}D_2E_2$
$a_{1,3}b_2c3d_4e_{1,3,4,5}$	$A_2B_1C_{1\text{-}2}D_2E_2$
Area 'Energy Security'	
$a_4b_2c_1d_7e_{1,2,3,5}$	$A_1B_3C_3D_2E_3$
$a_6b_1c_3d_7e_6$	$A_2B_1C_2D_{1\text{-}2}E_2$
Area 'Space'	
$a_4b_1c_2d_3e_1$	$A_2B_2C_1D_2E_2$
Area 'Solidarity/Defence'	
$a_{1,2,3,5}b_2c_2d_1e_{1,3,4,5,6,7}$	$A_2B_1C_{1\text{-}2}D_2E_2$
$a_3b_2c_3d_1e_1$	$A_2B_1C_2D_{1\text{-}2}E_2$

tise on specific aspects of the study that may not be available on the research team. Beyond the immediate impact, their participation strengthens networks, promotes the appreciation of foresight and thus facilitates decision-making on and the implementation of study results.

Acknowledgement: The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261633. 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. For more information visit the project website at www.focusproject.eu.

We acknowledge and express our gratitude to Australia's Defence Science and Technology Organisation, and the analyst Minh-Tuan Nguyen in particular, for kindly providing the Scenario Analysis Tool Suite. The provision of this tool suite made more efficient the scenario work performed by the Centre for Security and Defence Management within the FOCUS project.

Notes:

[1] Paul K. Davis, *Lessons from RAND's Work on Planning Under Uncertainty for National Security*, TR-1249 (Santa Monica, CA: RAND Corporation, 2012), quote on p. 1. www.rand.org/pubs/technical_reports/TR1249.html.

[2] See, for example, Michel Rademaker, "National Security Strategy of the Netherlands: An Innovative Approach," *Information & Security: An International Journal* 23:1 (2009): 51-61, http://dx.doi.org/10.11610/isij.2305; Sharon L. Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs* 1:2 (August 2005), www.hsaj.org/?article=1.2.2.

[3] Todor Tagarev and Petya Ivanova, "Expanded Capability Portfolios to Steer Force Development under Strategic Uncertainty," paper # 5 in Proceedings of the RTO SAS-072 Specialist Meeting on *Capability-Based Long Term Planning*, RTO-MP-SAS-072 AC/323(SAS-072)TP/240 (Oslo, 18-19 November 2008).

[4] For details see the Editorial to this I&S volume on "Scenario-based Security Foresight" by Prof. Alexander Siedschlag, http://dx.doi.org/10.11610/isij.2901.

[5] See *Problem space report: EU as a global actor based on the wider Petersberg Tasks*, FOCUS Deliverable 6.1, 27 January 2012, available at www.focusproject.eu.

[6] Adapted from Todor Tagarev, et al., *Methodology for Planning Wartime Defence Capabilities* (Sofia: Centre for Security and Defence Management, Institute of Information and Communication Technologies, 2012), p. 80. ISBN 978-954-91700-4-7. – in Bulgarian.

[7] The actual process has a number of feedback loops.

[8] See for example Tom Ritchey, "On the Formal Properties of Morphological Models," *Acta Morphologica Generalis* 1:2 (2012): 21-35, www.amg.swemorph.com/pdf/amg-1-2-2012.pdf.

[9] This is part of an established technique, known as *Battelle approach* and developed by the by Battelle Institute in Frankfurt. See Ute Hélène von Reibnitz, *Scenario Techniques* (New York, NY: McGraw Hill, 1985); Minh-Tuan Nguyen and Madeleine Dunn, *Some Methods for Scenario Analysis in Defence Strategic Planning*, DSTO–TR–2242 (Canberra: Defence Science and Technology Organisation, 2009), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA498161.

[10] Nguyen and Dunn, Some Methods for Scenario Analysis; Cigdem Dilek, *The Scenario Analysis Tool Suite: A User's Guide*, DSTO–GD–0560 (Canberra: Defence Science and Technology Organisation, 2009), www.dtic.mil/dtic/tr/fulltext/u2/a500350.pdf.

[11] For the rationale, advantages and the organisation of participatory foresight see for example *Handbook of Knowledge Society Foresight* (Dublin: European Foundation for the Improvement of Living and Working Conditions, 2003), www.eurofound.europa.eu/pubdocs/2003/50/en/1/ef0350en.pdf; Tuomo Kuosa, *The Evolution of Strategic Foresight: Navigating Public Policy Making* (Farnham, UK: Ashgate, 2012); and Ville Brummer, *Participatory Approaches to Foresight and Priority-Setting in Innovation Networks*, Doctor of Science dissertation (Espoo, Finland: Aalto University School of Science and Technology, 2010), http://urn.fi/URN:ISBN:978-952-60-3226-9.

[12] For details see FOCUS Deliverable 6.2 or Valeri Ratchev, Uwe Nerlich and Todor Tagarev, Context Scenarios and Alternative Future EU Roles as a Global Security Actor, *IT4Sec Reports* 100 (Sofia: Institute of Information and Communication Technologies, June 2012), http://dx.doi.org/10.11610/it4sec.0100.

[13] National Intelligence Council, *Global Trends 2030. Alternative Worlds* (Washington, D.C.: National Intelligence Council, December 2012), www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends.

[14] Envisioning 2030: US Strategy for Post-Western World (Washington, D.C.: Atlantic Council, December 2012), www.acus.org/files/publication_pdfs/403/Envisioning2030_web.pdf.pdf.

[15] Uwe Nelrich, "Towards Europe 2035 – In Search of the Archimedean Screw: FOCUS in Perspective," in this volume, http://dx.doi.org/10.11610/isij.2912.

[16] Details are provided in FOCUS Deliverable 6.1; and Todor Tagarev, Valeri Ratchev and Uwe Nerlich, Towards the exploration of future EU roles as a global security actor, *IT4Sec Reports* 92 (Sofia: Institute of Information and Communication Technologies, January 2012), http://dx.doi.org/10.11610/it4sec.0092.

[17] One of the working groups suggested three new roles.

[18] Uwe Nerlich, "Challenges in a 2035 perspective: Roles for the EU as a global security provider?," in this volume, http://dx.doi.org/10.11610/isij.2906.

TODOR TAGAREV, PhD, is Head of the IT for Security Department and the Centre for Security and Defence Management in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. He is Editor-in-Chief of *Information & Security: An International Journal*, www.procon.bg/infosec, and the DCAF series in Security and Defence Management. *E-mail*: tagarev@gmail.com

PETYA IVANOVA is CEO of Procon Ltd., www.procon.bg, and Associate Senior Fellow of the Centre for Security and Defence Management. She holds masters degrees in bioengineering, applied mathematics (both from the Technical University of Sofia) and decision support systems (University of Sunderland).