The FOCUS EU Security Foresight Project, its Embedded Scenario Method, and Bright and Dark EU Security Roles in a Horizon 2035 Futures Studies Tackling Wicked Problems: Where Futures Research, Education and Action Meet. 11-12 June 2015, University of Turku, Finland

Alexander Siedschlag
Professor & Chair of Homeland Security
The Pennsylvania State University
Background

- **Now:** Professor of Homeland Security and Chair of Penn State Homeland Security Programs

- **Was:** Professor of Security Research at Sigmund Freud University Vienna and Coordinator of the FP7 SEC project FOCUS: Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles

- **Interested in:** Maintaining the FOCUS momentum and the projects contribution to the impact of foresight studies on homeland and civil security research and policy planning
Presentation overview

- FOCUS project and embedded scenario method
- Theme: EU as a Global Actors as example
- FOCUS scenario information and portfolio integration framework and road map
- FOCUS output structure and impact framework
- Types and uses of FOCUS (dark) scenarios
FOCUS project outline

- **Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles (2011-2013)**

- **13 partners from 8 countries** (AT, BE, BG, CH, CZ, DE, ES, IL) – big industry, SME, academia, and think tank + **End-user Test & Evaluation Panel**

- Shape European security research to enable the EU to effectively respond to tomorrow's challenges stemming from the globalization of risks, threats and vulnerabilities.

- Concentrate on alternative future EU roles to prevent or respond to incidents situated on the "borderline" between the internal and external dimensions of the security affecting the Union and its citizens.

- Elaborate multiple scenarios, based on IT-supported foresight, in the form of alternative futures, on order to increase the EU’s requisite variety for coping with relevant alternative futures in the 2035 time frame.

- Deliver tangible products (such as an IT-based Knowledge Platform) and contents (e.g., a roadmap) for planning research and deciding on priorities.
FOCUS foresight

- “Scenario foresight”: Foresight presented in the form of scenarios.
- “Embedded scenario” approach: Alternative futures of security research in the context of future EU roles.
FOCUS’ five big themes ("2035")

- Different tracks regarding the future of the **comprehensive approach** as followed by European institutions, Member States, and international strategic actors – including links between the internal and external dimension of security.

- **Natural disasters and environment-related hazards**, with an emphasis on comprehensive risk reduction, civil protection, and reconstruction.

- **Critical infrastructure and supply chain protection**, centred on preventing, mitigating, and responding to exogenous threats that could have a significant impact on EU citizens.

- The **EU as a global actor**, building on EU-level and Member States instruments and capability processes as well as on effective multilateralism.

- The evolution of the **EU’s internal framework** and prerequisites for delivering a comprehensive approach, including strategies for engagement with other international actors, ethical acceptability, and public acceptance of future security roles of our Union.
FOCUS scenario foresight in figures

- Scenario foresight in FOCUS included a broad number of different types of experts and stakeholders, and a variety of scenario information (such as online and on-site questionnaires, new social media information, workshops, studies, related projects’ results, etc.).
- In total (online and on site), FOCUS involved more than 600 external experts and end-users from more than 20 countries, both within and beyond the EU.
- Experts and end-users were identified in horizon scanning, in scanning of related projects, and by using partners’ lists of experts.
- Participating experts and end-users represented EU bodies, national federal bodies and international bodies, industry, first responder organizations, think tanks, universities, NGOs, and other sectors.
- As far as its on-site work is concerned, FOCUS held more than 40 external and more than 30 internal foresight workshops.
“EU 2035” role scenarios for the “EU as a Global Actor” theme

 Proper EU roles:
• Blue cross: the EU as a global civilian crisis management actor
• Nolens volens: the EU as a compelled globalist
• For your eyes only: towards an EU regional security and defence policy
• Happy together: towards a multilevel framework of cooperation
• Blue bull: towards an EU global security and defence policy
• Lonely star: renationalization of security and defence

Selected as context scenarios (highest combination of probability/likelihood and impact):
• “Nolens volens”
• “For your eyes only”
Selected conclusions from problem space description

- The concept of the global European power should address in a suitable way the basic EU characteristics in order to provide the most relevant package of power components to every particular case of engagement.

- The extreme dark scenario would be foreign and security policy and actions undertaken in a way that, while maximizing one type of effect (e.g. the military effect), damages the most positive one: the social attractiveness of EU.

- Instruments of EU global roles may include increased justice and law enforcement capabilities; increased EU intelligence and early warning capabilities; financial instruments for influencing economic developments on a global scale; good governance and institution building; or civil society-related and cultural instruments, including media, social networks, etc.

- Caveat: Other dark scenarios would include oversophisticated capabilities, overstretch of the European Security Model, or a self-serving comprehensive approach.
When will security cooperation work?

Classic example:
Holsti: Unity and Disintegration in International Alliances (1973)

Predictors for Alliance Cohesion

- Is an Alliance able to find a common denominator of its objectives among its member states and to take common action to realize those objectives?

- Example: Negative predictors for alliance cohesion
  - Status inconsistency (self image vs. perceived role)
  - Sub-alliances (e.g., old vs. new Europe, haves and have-nots, etc.)
  - Incompatibility of capabilities
  - Divergent perceptions/assessments of external threats
# Main drivers for EU roles

<table>
<thead>
<tr>
<th>1.</th>
<th>Extent of information and intelligence sharing, and early warning capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Convergence or divergence of security cultures</td>
</tr>
<tr>
<td>2. (same ranking)</td>
<td>Politics of multilateral partnerships against global security threats</td>
</tr>
<tr>
<td>2. (same ranking)</td>
<td>Practical strength of the “European Security Model,” as advocated in the EU Internal Security Strategy: addressing the causes of insecurity and not just the effects; prioritizing prevention and anticipation, and involving all sectors with a role to play in public protection (political, economic, social, etc.)</td>
</tr>
<tr>
<td>3.</td>
<td>Asymmetry of security capabilities of Member States, the EU and adversaries</td>
</tr>
<tr>
<td>3. (same ranking)</td>
<td>Science and technology innovation</td>
</tr>
<tr>
<td>3. (same ranking)</td>
<td>Societal resilience</td>
</tr>
<tr>
<td>4.</td>
<td>Changing national security capacities and levels of asymmetry (relative difference between the capacity of nations to influence security affairs)</td>
</tr>
<tr>
<td>4. (same ranking)</td>
<td>Development of common strategic culture and cooperative spirit</td>
</tr>
<tr>
<td>4. (same ranking)</td>
<td>Whole of community approach based on technological facilitation and empowerment, in particular new social media applications for crowd sourcing/mapping in developing operational pictures</td>
</tr>
</tbody>
</table>
Scenarios for “Security Research 2035” on the EU as a global actor

- “Hands across the ocean” – Using multilateralized technologies to countering cyber threats
  RESEARCH ON COUNTERING CYBER THREATS IN A COOPERATIVE ENVIRONMENT

- “Waterworld” – Corporate autarchy and maritime security
  RESEARCH ON MANAGING MARITIME CRISES IN A HIGHLY COMPETITIVE ENVIRONMENT

- “Every nation is an island” – Only national policy drives the CBRN agenda
  RESEARCH ON MANAGING CBNR CRISES IN A NATIONALIST ENVIRONMENT

- “Back to the future” – Multilateral structures to contain conflicts
  RESEARCH ON MANAGING SUPPLY CHAIN DISRUPTIONS IN A WORLD DOMINATED BY INGOS (INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS)
Reference scenario for the Big Theme: “EU 2035” as a global actor

- “Borderless Threats = Mission Creep” –
  The EU’s forced march toward a stronger Common Security and Defence Policy
  - The EU’s policy to counter cyber-attacks is paramount since this form of societal defence has become all-encompassing for Europe’s economic, industrial and scientific development.
  - A strong transatlantic framework of homeland cooperation has emerged by 2035, though it is geared towards joint pragmatic/operational action, but not necessarily towards joint technology development.
  - Main EU role aspects (mission scenario aspects):
    - EU action across crisis management cycle and internal-external security continuum
    - Increased dependence and vulnerability of maritime security
    - Cyber security is key: continuous cooperative vulnerability assessments
    - Risk of over-sophisticated capabilities
  - Main RTD aspects (security research scenario aspects)
    - Technology assessment expertise
    - Simulation capabilities
    - Trade-off between EU global engagement and EU public protection and development
    - Security economy: reduce costs of security
    - Defence-security continuum
    - Non-technological security tracks: financial instruments, industrial strategies, resilience gaps
Main reference scenario drivers

- Comprehensive (societal, economic and institutional) resilience to crises and disasters
- Science and technology innovation
- Practical strength of the “European Security Model” as advocated in the EU Internal Security Strategy: addressing the causes of insecurity and not just the effects; prioritizing prevention and anticipation, and involving all sectors with a role to play in delivering security to citizens
- Asymmetry of capabilities of Member States, the EU and adversaries – including regionalization vs. globalization of security
- Extent of information and intelligence sharing, and early warning capabilities – including policies for information exchange
- Decision-making tools based on joined-up situation analyses, including their use to secure public acceptance and support
<table>
<thead>
<tr>
<th>Threat/challenge</th>
<th>Technology/capability (need)</th>
<th>Research need</th>
<th>Ethics aspects implied by research need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber attacks</td>
<td>Cooperative vulnerability assessment</td>
<td>• Modelling &amp; simulation (incl. of societal aspects)</td>
<td>• involves linking of data, data merger or data analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modern governance and social engineering</td>
<td>• facilitates societal security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resilience</td>
<td>• aims to combat terrorism</td>
</tr>
<tr>
<td>CBRN, in combination with failed states</td>
<td>• CBRN protection • Surveillance, incl. space-based</td>
<td>• Control of pandemics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Measures against nuclear threat</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Space satellites</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unmanned platforms</td>
<td></td>
</tr>
<tr>
<td>Disruption of supply chains</td>
<td>Intelligence sharing</td>
<td>• Enhanced interoperability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exogenous (remote/“stand-off”) attacks on technological systems (critical infrastructures)</td>
<td>External threat detection/early warning</td>
<td>• Real time Intelligence</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• involves linking of data, data merger or data analysis</td>
</tr>
<tr>
<td>Maritime crises</td>
<td>Common operational picture</td>
<td>• International collaborative training</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• involves linking of data, data merger or data analysis</td>
</tr>
<tr>
<td>Supply chain disruption</td>
<td>• Protection of IT and communications systems and networks (cyber security) • Recovery of critical infrastructures Consequence management</td>
<td>• Cyber security International collaborative training</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resilience</td>
<td>• facilitates societal security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• involves linking of data, data merger or data analysis</td>
</tr>
<tr>
<td>FOCUS five “Big Themes”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Comprehensive approach</strong></td>
<td><strong>Natural disasters &amp; global environmental change</strong></td>
<td><strong>Critical infrastructure &amp; supply chain protection</strong></td>
<td><strong>EU as a global actor based on the wider Petersberg Tasks</strong></td>
</tr>
<tr>
<td>Common scenario foresight methodology and strategy for integration of results</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foresight tool repertory (identification, summary and assessment of publicly available tools)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Working version of IT-based Knowledge Platform, with “scenario tools workbench” as current front end and definitions of scenario foresight processes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental scanning and problem space description</td>
<td>Environmental scanning and problem space description</td>
<td>Environmental scanning and problem space description</td>
<td>Environmental scanning and problem space description</td>
</tr>
<tr>
<td><strong>Summary of problem space descriptions with proposed cross-cutting key drivers</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Syllabus of scenarios for “EU 2035” security roles</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Thematic scenario portfolio for “Security Research 2035”</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation of results in the further development of the IT-based Knowledge Platform</td>
<td>Implementation of results in the further development of the IT-based Knowledge Platform</td>
<td>Implementation of results in the further development of the IT-based Knowledge Platform</td>
<td>Implementation of results in the further development of the IT-based Knowledge Platform</td>
</tr>
<tr>
<td>Addressing of cross-cutting aspects and capabilities, including ethics issues (with some cross-theme foresight work)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Comprehensive scenario assessment questionnaire and total assessment of scenario drivers</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information, results and requirements from related projects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plausibility probe and input into reference scenario process</td>
<td>Plausibility probe and input into reference scenario process</td>
<td>Plausibility probe and input into reference scenario process</td>
<td>Plausibility probe and input into reference scenario process</td>
</tr>
<tr>
<td>Plausibility-probed reference scenario syllabus with wiki implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-user memorandum on/evaluation of the reference scenarios</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOCUS conclusions for “Security Research 2035”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOCUS roadmap proposal for the planning of “Security Research 2035,” including a public “light” version implemented on the final version of the IT-based Knowledge Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
FOCUS output structure/impact model

Roadmap for the planning of “Security Research 2035” as a paradigm combining elements of “technology roadmap” and “balanced scorecard” type

**Horizontal dimension**
- time line: immediate action, short-term, mid-term, long-term

**Vertical dimension**
- Reference scenario aspects - "pull" factors, where futuristic scenarios require certain types and efforts of security research
- General aspects - "push" factors, where certain general requirements for and expectations from security research drive the future development

**IT-based Knowledge Platform**
- Process stepper
- Big themes & thematic scenario wikis
- Reference scenario wikis
- European Security (Research) Glossary
- Curriculum matrix/qualification profile
- Tools & questionnaires repository

**Reference scenarios (planning scenarios)**

**Scenarios for “Security Research 2035” to support “EU 2035” security roles**

- Problem space descriptions/project studies
- Horizon scanning/related projects

**Scenarios for “EU 2035” security roles**

Sustainability framework for FOCUS methodology, tools, content and results
Population with FOCUS results for their comprehensive accessibility
Multiple (multi-step, multi-method, multi-source scenario foresight process)
FOCUS “impact products”

<table>
<thead>
<tr>
<th>Studies</th>
<th>Roadmap “Security Research 2035”</th>
<th>Website and New Social Media sites</th>
<th>IT-based Knowledge Platform</th>
<th>… with wikis and tools, to be opened for external contributions</th>
<th>Journal special issue</th>
</tr>
</thead>
</table>

- **Studies**
  - Roadmap “Security Research 2035”
  - Website and New Social Media sites
  - IT-based Knowledge Platform
  - … with wikis and tools, to be opened for external contributions

**FOCUS – Foresight Security Scenarios**
FOCUS IT-based knowledge platform (example)

Security Research 2035 Reference Scenarios Wiki
This Wiki explains the reference scenarios for the planning of Security Research in the 2035 time frame that FOCUS derived from IST thematic scenario syllabi.
The FOCUS Roadmap is calibrated towards those reference scenarios and their identified indicators. These scenarios are public domain and free for use by projects, agencies, etc. to broaden knowledge base of the “Security Research enterprise” and related policies.

Scenario Syllabus Wiki
This Wiki contains all thematic scenarios developed by FOCUS based on its multiple foresight process. These scenarios comprise two levels, which both reflect the 2035 time frame of the FOCUS Roadmap.
1. Scenarios for roles of the “EU 2035” as a security provider, including futuristic mission scenarios;
2. Scenarios for alternative futures of “Security Research 2035” that delivers knowledge, products, and services to support those “EU 2035” roles.
These scenarios are public domain and free for use by projects, agencies, etc. to broaden the creative knowledge base of the “Security Research enterprise” and related policies.

European Security Research Glossary Wiki
This Wiki contains the glossary of terms, abbreviations and concepts compiled by FOCUS as they appear relevant to EU security roles and Security Research today and in the 2035 timeframe of FOCUS foresight.

FOCUS Method Wiki
This wiki carries information of the FOCUS Method, on foresighting, and on developing scenarios. Apart from providing basic information, it aims to make experience from the FOCUS project and subsequent projects as well as interested experts and researchers who intend to conduct scenario foresight.
FOCUS roadmap proposal for multi-tier planning of “Security Research 2035”

http://www.focusproject.eu/knowledgeplatform/workbench
Best practices, issues, and lessons learned in scenario development

Practical aspects:
- Good experience with anonymous online questionnaires.
- Limited reaction on attempts to spark scenario discourse in New Social Media, although information though these channels is taken on (not ignored).
- Diverse regional coverage easier to achieve than target turnout figures.
- Foresighted “security stakeholders 2035” are not always aware/prepared to accept they may be going to be stakeholders.

Scenario method aspects:
- Cross-referencing approach and multiple plausibility probe.
- **Normativism within the team; intentions to “sell” the “right” future.**
- Mix-up between futuristic scenarios and mission scenarios.
- Fallacy of basing scenario thinking in a 2035 time frame on postures (strategies & capabilities) of today.
Uses of dark scenarios from FOCUS

- Helps prevent methodological fallacies (e.g., normativism)
- Highlighting of risks and vulnerabilities
- Focusing on “gaps” and how to close them; emphasis on capability gaps
- Awareness for self-contradictory EU role patterns
- Scenario drivers from bright to dark and vice versa
- “Right” security research for the “wrong EU”
- “Wrong” security research for the “right” EU
- Supports security research core approach
Security research core approach

- Analysis of a part of society and its material (e.g. critical infrastructure) and non-material (e.g. resilience) foundations
- Identification of risks and threats to which the object of analysis is exposed
- Identification of security gaps, or needs for asset protection
- Development of research questions based on the identified gaps; typical topics include:
  - Harmonization of different security systems
  - Collaboration at system transition points (such as public – private, internal – external, and other security continua)
  - Distribution effects of security interventions
  - Citizen acceptance of security technologies and interventions
  - Early identification/warning of security gaps – anticipatory security governance
- Prioritization by negative security impact of each gap
- The objective is to develop capabilities to close the security gaps

FOCUS was co-funded by the European Commission under the 7th Framework Programme, theme "security", call FP7-SEC-2010-1, work programme topic 6.3-2 "Foresighting the contribution of security research to meet the future EU roles", Grant Agreement no. 261633.
Contact

Alexander Siedschlag, Ph.D.
Professor of Homeland Security
Chair, Intercollege Master of Professional Studies Program
in Homeland Security

The Pennsylvania State University -- Penn State Harrisburg
School of Public Affairs
160W Olmsted Building
777 West Harrisburg Pike
Middletown, PA 17057

Phone (717) 948-4326 (Program Office: 6322) -- Fax (717) 948-6484

http://harrisburg.psu.edu/programs/master-homeland-security

Like iMPS HLS on Facebook! -- http://www.facebook.com/PSU.HLS