The FOCUS Project (04/2011-03/2013)
Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles

FOCUS
FP7-SEC-2010-1

ARCHIMEDES Roundtable

"External Dimension of Security: EU Science and Technology"

Brussels, 24-25 April 2013

Foresight Security Scenarios

Alexander Siedschlag

CEUSS | Center for European Security Studies
Sigmund Freud University Vienna

FOCUS objectives

- Help 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.
- Do so by elaborating multiple scenarios, based on IT-supported foresight, in the form of alternative futures that are plausibility-probed and not mere threat scenarios.
- Develop an effective long-term foresight and assessment tool at the EU level, populated with the analyses carried out by the project.

FOCUS consortium & main steps

- FOCUS united **13 partners** from **8 countries** (AT, BE, BG, CH, CZ, DE, ES, IL) – big industry, SME, academia, and think tank.
- FOCUS undertook **multiple scenario foresight,** done on the level of strategic forward thinking in order to increase the EU's requisite variety for coping with relevant alternative futures in the **2035 time frame.**
- FOCUS first developed roles of the **"EU 2035"** as a comprehensive security provider.
- These role sets were then used as context scenarios for deriving alternative futures of **"Security Research 2035**" that supports the EU roles.
- Both levels of insight were then integrated into **reference scenarios,** based on which **roadmapping** was done.
- Scenarios were developed based **on IT-supported foresight,** in the form of **plausibility-probed alternative futures.**

FOCUS scenario foresight facts

- 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 **670 external experts and end-users from 24 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.**

FOCUS' five Big Themes

- 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 as well as ethical acceptability and public acceptance of future security roles of our Union.

FOCUS output structure

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

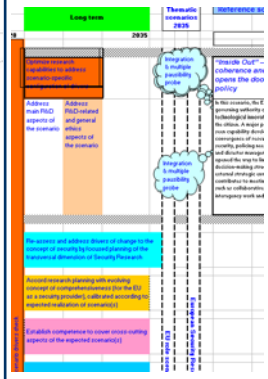
Scenarios for "EU 2035" security roles

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 products for further use

Studies	Road-map “Security Research 2035”	Website and New Social Media sites	IT-based Know-ledge Platform	… with wikis and tools, to be opened for external contributions	Journal special issue
					

Selected FOCUS foresight results from relevant “Big Themes” in the 2035 time frame

- Drivers
- Thematic scenarios
- Reference scenarios
- Technology aspects
- Needed investments
- Security research topics

Drivers of change to the concept of security in the “EU 2035”

- **Crises** resulting from scarcity of resources;
- **Evolution of the need for societal resilience and preparedness;**
- **Changing borderlines between internal and external security;**
- **Technological change,** driving or changing security needs
- **Mass migration flows;**
- New potentials and profiles of **international conflicts** with main leverages like cyber; energy; scarce resources; etc.;
- **Diffusion of power** within and among nation-states;
- **Dependency on information and communication technology,** and technology in general (with risk of cascading breakdown of systems)
- **Demographic shifts** with pressure on resources;
- **Increased reliance on critical infrastructures that are vulnerable and have little spare capacity,** operate at the edges of performance and loads, are critically depending on other infrastructures.

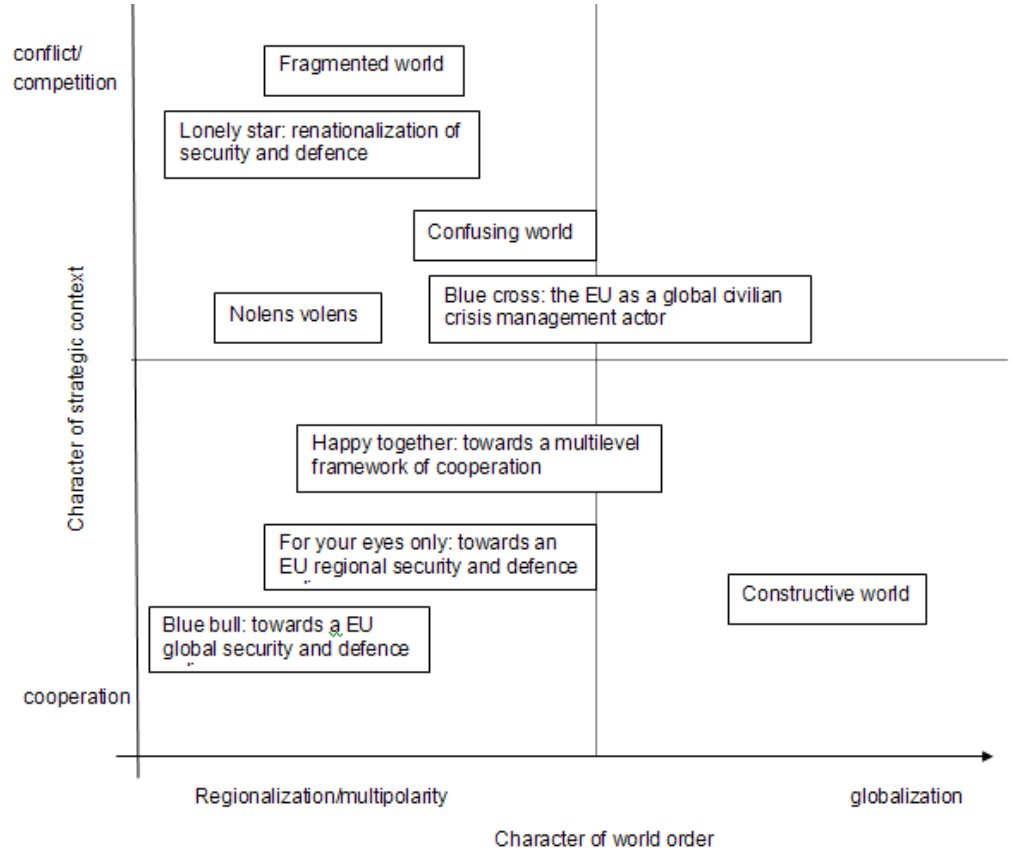
Main drivers for “EU 2035” external roles

1. Extent of information and intelligence sharing, and early warning capabilities
2. Convergence or divergence of security cultures
2. (same ranking) Politics of multilateral partnerships against global security threats
2. (same ranking) 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 relevant sectors (political, economic, social, etc.)
3. Asymmetry of security capabilities of Member States, the EU and adversaries
3. (same ranking) Science and technology innovation
3. (same ranking) Societal resilience
4. Changing national security capacities and levels of asymmetry (relative difference between the capacity of nations to influence security affairs)
4. (same ranking) Development of common strategic culture and cooperative spirit
4. (same ranking) Whole of community approach based on technological facilitation and empowerment, in particular new social media applications for crowd sourcing/mapping in developing operational pictures

Selected conclusions from FOCUS problem space descriptions

- 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 negative example could be when foreign and security policy and actions are undertaken in a way that, while maximizing one type of effect (e.g. the military effect), could damage the most positive one: the social attractiveness of EU.
- The application of the comprehensive approach should not be understood as a practice only, but also as a conceptual ground for the EU global power.
- Instruments of “EU 2035” 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, including in security sectors; or civil society-related and cultural instruments, including media, social networks, etc.

Scenarios for “EU 2035” external roles



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 a 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”*

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 CBNR 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

Reference scenario "Comprehensive Approach 2035"

- **"No Land is an Island: A protected EU homeland with external responsibilities"**
  - In 2035 the EU and its Member States have developed a common model that guides security policy along the internal–external continuum. It rests on a much closer integration of national Security Research programmes with that of the EU.
  - While the EU prides itself as an "open" system that accords respects for a multilateral world, its Security Research system is largely homeland-focused and geared to coping with security threats to the Union's own territory.
  - Security Research has contributed to commonly-owned European security assets and capabilities that evolve from public-private cooperation. These are partly shared by civil and military actors.
  - Internally, the EU has substantially expanded its early-warning capabilities and rapid-alert systems regarding civil threats.
  - Externally, the EU's comprehensive approach is basically one of coordinating autonomous actors who share information and pool resources due to domestic budgetary restrictions.

Main reference scenarios drivers regarding the external dimension

- 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 public protection;
- 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.

Main technology aspects identified

- Knowledge management for comprehensive situational awareness;
- Meta-technology to collect, integrate, and comprehensively use data and information from different sources to allow for more informed decisions;
- Syllabi of mechanisms of external threats, such as on EU critical infrastructure, mainly related to information and ICT, and cyber attacks;
- Platform technology for structured information exchange (e.g. inter-agency) and information interoperability;
- Vulnerability and response capabilities simulation;
- Platforms for education and training;
- Mobile broadband communication : exchange of information over long-distance in real time, with high quality and reliability ;
- RPAS;
- Imaging;
- Sensoring, both substance and intelligence-related (e.g., web search instruments) .

The challenge of managing larger expectations with fewer resources

- As an analogy to NATO's concept of "smart defence" for allied procurement, future security research may help develop a smart approach in terms of a hazard-driven policy and capability process, based on integrated assessment and decision-making that transcends the security–safety divide and broadens EU and Member States security strategies to encompass both.
- The lead strategy, however, will be a civil one: to link EU "coping capabilities" with citizen resilience.
- There is a risk of the EU developing over-sophisticated capabilities, since discussions of effects-based approaches to comprehensive security could result in a more politically than strategically defined level of ambition on the side of the EU and its Member States, with capabilities developed that sometimes have limited effects on the real security challenges at hand.

Main needed investments in the light of FOCUS scenarios & drivers

- Big data information management and information integration to ensure sustainable cooperation between all actors involved;
- Interoperability and coordination related to information and communication technology – between and within international organizations;
- International programmes to contain epidemics in their regions of origin, keeping them from reaching EU territory;
- Preventive and integral medicine;
- Non-military instruments for EU power projection, such as financial instruments;
- Improved technology for identification of vulnerabilities and gaps of resilience, and integration of relevant information.

FOCUS recommendations for future research topics

- Implementation of the comprehensive approach, including strategies, capabilities, instruments, and security communities; the latter should cover the levels of commitment and asymmetries of the Member States and the EU, their abilities and instruments, and their “strategic cultures” and world views.
- Corresponding capability-related challenges, such as the following:
  - Capabilities that can impact from any distance (advanced drones, other advanced robotics systems, strategic cyber capabilities, space capabilities, etc.);
  - Capabilities that can disrupt external EU lifelines (energy, communication, etc.);
  - Changing economic and financial leverage that can have negative or positive impacts on security challenges to the EU; challenges that result from differentials in the EU’s wider neighbourhood (population, age, employment, competence, etc.).

http://www.focusproject.eu

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 “Fore sighting the contribution of security research to meet the future EU roles”, Grant Agreement no. 261633.