

 Content archived on 2024-06-18



Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles

Reporting

Project Information

FOCUS

Grant agreement ID: 261633

[Project website](#) 

Project closed

Start date
1 April 2011


End date
31 March 2013



Funded under
Specific Programme "Cooperation": Security

Total cost
€ 4 523 049,67

EU contribution
€ 3 407 075,80

Coordinated by
SIGMUND FREUD
PRIVATUNIVERSITAT WIEN
GMBH
 Austria

Final Report Summary - FOCUS (Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles)

Executive Summary:

FOCUS ("Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous

EU Roles”) helped shape European security research to enable the EU to effectively respond to tomorrow’s challenges stemming from the globalisation of risks, threats, and vulnerabilities. FOCUS concentrated 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. It did so by elaborating multiple scenarios, based on IT-supported foresight, in the form of alternative futures. These were rooted in threat integration and a comprehensive approach to future missions to provide security to the Union and its citizens.

FOCUS identified and assessed alternative sets of future tracks for security research in FP7 and subsequent programmes that will support the EU to adopt new roles in dealing with external threats, risks, and vulnerabilities. The main contribution of the FOCUS project was the development of an effective long-term prediction and assessment tool at EU level, populated with analyses done in the project. The time frame of scenario foresight in the FOCUS project was 2035.

FOCUS provided studies, security scenarios, roadmaps, and an IT-based Knowledge Platform for scenario foresight, with the latter offering a large number of practical tools such as scenario wikis, reference wikis, and a curriculum matrix for educating future security researchers.

New stakeholders of security research will comprise security forces other than military, for example public entities such as national and possible emerging EU customs and border protection, other national and international security agencies, as well as private entities. Stakeholders will moreover come from the banking, finance, economic, and health sectors. Other international organisations and NGOs will be stakeholders in European cross-disciplinary security research. With the concept of societal security increasing in importance, national and international non-profit civilian organisations will develop increasing stakes in security research.

Security research will contribute to improving an EU-specific legal compliance framework to collectively support and protect the security and safety of EU citizens against external impacts. Progressive standards and codes of conduct will be critical for enabling the EU to implement responsible technology governance. At the same time, multidisciplinary mapping of fundamental rights enforcement and the acceptability of security technologies and interventions will become paramount across the EU Member States.


Becoming both a more policy-informing and societally embedded enterprise, future security research will always face the problem of having to meet larger expectations with fewer resources. Discussions of effects-based approaches to comprehensive security, as applied to home affairs, will 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.

Investments in the field of big data information management and information integration will be needed to ensure sustainable cooperation between all actors involved. Moreover, additional investments in interoperability and coordination related to information and communication technology, – between and within international organisations – will be required. Investments will also be required in the sector of non-military instruments for EU power projection, such as financial instruments, as well as on industrial strategies and identification of vulnerabilities and gaps of resilience.

Project Context and Objectives:

FOCUS (“Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles”) aimed 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.

During the times of manifest Cold War threat scenarios, Arnold Wolfers, professor and expert in international relations, complained that “national security” was a symbol that left too much room for confusion to serve as a guiding principle for political advice or scientific analysis (A. Wolfers: “‘National Security’ as an Ambiguous Symbol,” *Political Science Quarterly* 67:4 [December 1952]: 481-502, quote on p. 483). He suggested that, as a first step in developing an analytical concept of the term, security should be considered, “in an objective sense, [...] the absence of threats to acquired values, [and] in a subjective sense, the absence of fear that such values will be attacked.” (ibid., p. 485)

After the end of the Cold War, security policy continued to be understood as a normative practice, namely as defending values (B. Buzan: *People, States, and Fear*. Boulder, CO: Rienner, 1991). The notion of security as a value-laden concept and its essential link to society has been taken up by the new field of security research, which includes a focus on “societal security” in addition to – or beyond – the security of infrastructures, utilities, etc. Security research aims for a comprehensive approach to delivering security (including civil protection) to the citizens – by civil means and without infringing individual rights and freedoms (cf. European Societal security research Group, <http://www.societalsecurity.eu> .

The main focus of security research, however, has been on technological solutions for security problems and their thorough check for social and ethics issues, such as the acceptability and impact on citizens’ perception of (in)security. This must be an integrated part of the research process. Reaching beyond this state of the art, what has been termed “new security studies” (cf. J.P. Burgess, ed.: *The Routledge Handbook of New Security Studies*. Milton Park: Routledge, 2013) aims to integrate concepts and approaches from classical, strategic security studies, and security research.

Embracing academic perspectives within the spectrum of “new security studies” and those from industry and end-users, FOCUS aimed to contribute toward shaping research to enable the EU to effectively address future challenges to comprehensive security. The main idea of FOCUS was to develop multiple scenarios that function as common denominators for challenges (involving new tasks) whose causes are external to the territory of the Union, but whose consequences will be experienced on the territory of the Union and EU responses using tangible contributions from security research.

By extrapolating the Member States’ prerogative over security on the national scale, the Lisbon Treaty (2009) introduced the concept of the security of the European Union (EU) itself: Based on its new legal personality, the Union now aims “to promote peace, its values and the well-being of its peoples” (Article 3 Treaty on European Union). For the security of the Union and its citizens, it is the Union that “shall define and pursue common policies and actions, and shall work for a high degree of cooperation” (Article 21).

The Lisbon Treaty also effected a significant transition towards harmonisation in the field of civil protection

against natural or anthropogenic (or “man-made”) disasters: The Union now has the competence to support, coordinate, and/or complement the actions of the Member States (Article 196 Treaty on the Functioning of the European Union).

In total, the Treaty on European Union in the Lisbon version establishes the Union as a whole as a security provider to its citizens, reaffirming its role as a global actor, based on collective European values and security interests: “In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens” (Article 3 Treaty on European Union).

Still mirroring the pre-Lisbon Treaty state of play, however, the current state of security research in Europe is characterized by national focuses on a limited number of pre-defined missions or parallel scenarios that typically result from an analysis of specific national incidents, requirements, or shortcomings. By contrast, FOCUS elaborated foresight-generated multiple scenarios for EU security roles and related security research topics, approaches and structures to introduce scenario planning from a European perspective, and to broaden the concept of security research.

The work of FOCUS seeks to assist the EU, its Member States, industry, and other stakeholders to design a common approach to the contribution of security research to effectively cope with challenges arising from the globalisation of risks, threats, and vulnerabilities before they deplete the EU’s ethical and societal legitimacy as a comprehensive security provider for its citizens.

FOCUS was co-funded under the security research theme of the EU’s Seventh Framework Programme (FP7), for the period of April 2011 to March 2013. The project brought together 13 partners from eight countries, including universities, industry, think tanks, and security information providers. FOCUS successfully replied to the following topic:

Topic SEC-2010.6.3-2 Fore sighting the contribution of security research to meet the future EU roles

New tasks are expected to strengthen the EU’s role towards providing a comprehensive security approach to its citizens. The external dimension of security may become every more important. The security impact of global climate change needs to be addressed. Furthermore, a stronger common approach to civil protection and crisis management is needed. The task is to develop scenarios as how security research under FP7 and beyond can best contribute to this comprehensive approach while giving due consideration to the ethical and societal dimension.

Expected impact: Provide input for the planning of security research to meet future EU roles beyond those defined in the ESRAB report.

FOCUS was a scenario foresight project. Foresight is a participatory approach to strategic forward thinking to increase the requisite variety to cope with alternative futures in a world to come. The FOCUS project had a 2035 time frame. Foresight neither predicts the future, nor circumscribes normative desirable futures or “wishful thinking.” Foresight is about describing different possible futures. It is calibrated to

diversity, not to delimitation.

Results and insights of foresight can be presented in different ways. One common way is to present foresight results in the form of scenarios. A scenario is

“a ‘story’ illustrating visions of a possible future or aspects of a possible future. It is perhaps the most emblematic foresight or future studies method. Scenarios are not predictions about the future but rather similar to simulations of some possible futures. They are used both as an exploratory method and as a tool for decision-making, mainly to highlight the discontinuities from the present and to reveal the choices available and their potential consequences.” (European Commission Joint Research Centre: “Scenario Building. Definition” (2006), http://forlearn.jrc.ec.europa.eu/guide/2_scoping/meth_scenario.htm#Definition [last access: 12-03-2013]).

As foresight itself, thus, the scenarios that it yields include thinking in extremes, low probability/high impact aspects, etc. The scenarios are not master plans, policy recommendations, or suggested normative trends.

The FOCUS foresight approach departed from institutional Europe as defined through the Lisbon Treaty. Within a 2035 time horizon, a scenario-approach was chosen that allows the identification of threats and incidents that may affect Europe, required responses, and eventually European futures. FOCUS concentrated 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. It did so by elaborating multiple scenarios, based on IT-supported foresight, in the form of alternative futures. These were plausibility-probed versus mere threat scenarios.

The main contribution of the project is the development of effective long-term prediction and assessment tools at the EU level. Overall, FOCUS followed six objectives, each building upon each other, namely to:

- Identify alternative sets of future tracks for security research in FP7 and subsequent programmes, supporting EU roles to deal with exogenous threats, risks, and vulnerabilities.
- Elaborate on the concept of transversality in assessing evolving needs for research across traditional disciplines, presently defined mission areas and throughout the security continuum.
- Design and apply a specific scenario approach (“embedded scenarios”). This was based on foresight to ensure openness, participation, and inclusiveness (e.g. involvement of societal stake-holders), while explicitly addressing security perceptions and security in relation to other values.
- Produce an IT information infrastructure (by adapting existing information technologies) that will make material and tools for scenario planning of security research available to knowledge communities.
- Enhance transparency, improve understanding, and increase preparedness for the emerging challenges of the “external dimension” and the “external–internal continuum” of security and the evolution of security research.

- Contribute to the planning of security research beyond the European security research Advisory Board (ESRAB) and European security research and Innovation Forum (ESRIF), based on foreseen EU roles rather than on pre-defined missions.

Approaches and results from the FOCUS project revolve around the planning of security research in the 2035 time frame to support foresighted EU security roles. In a follow-up, they could be carried further to help provide a framework for analyzing long-term trends and dynamic interactions in a global environment undergoing tectonic changes, reaching beyond the FOCUS mission to explore new contexts of security research in support of possible future EU role scenarios. European developments are in large part driven by challenging global developments, reaching beyond external risks and threats to which the EU needs to respond (see European Commission: Global Europe 2050. Luxembourg: Publications Office of the European Union, 2012).

Project Results:

1. FOCUS method

1.2 Five “Big Themes”

FOCUS conducted foresight on an inclusive basis, making maximum use of its IT support for integration of multiple stakeholders, experts from a broad range of fields, and the interested public to address security in relation to other societal as well as ethical values. This approach was especially important in the context of scenario planning in order to ensure that the selected policies and security technologies were responsive to the needs of citizens and that they created security approaches rooted in acceptance.

Scenario foresight in the FOCUS project was carried out via critical and creative – yet methodologically guided – forward thinking at the strategic level, aiming to increase the EU’s ability to cope with relevant alternative futures from the near future until 2035.

This task was performed along the following five “Big Themes” as derived from environmental scanning and research done in preparation of the project:

- Comprehensive approach: Alternative future tracks in further developing the comprehensive approach as followed by institutions and states, including links between the internal and external dimension of security.
- Natural disasters and global environmental change: Scenarios for future EU roles in preparing for and responding to natural disasters and environment-related hazards, focused on comprehensive crisis management.
- Critical infrastructure and supply chain protection: Scenarios for future EU roles centred on preventing, mitigating, and responding to exogenous threats that could have a significant impact on EU citizens.
- EU as a global actor: Alternative futures of the EU as a global actor based on the wider Petersberg tasks, building on EU and Member States instruments and capability processes.

- EU internal framework (and EU homeland security): Scenarios for the evolution of the EU's internal framework and prerequisites for delivering a comprehensive approach, including Lisbon Treaty provisions and relevant strategies (e.g. for engagement with other international actors) as well as ethical acceptability and public acceptance.

1.2 “Embedded scenario” method

The FOCUS approach presented the results of the performed foresight on three scenario levels:

- First, scenarios for “EU security roles” in the up to 2035 time frame;
- Second, within those context scenarios for EU roles, scenarios for alternative futures of “security research 2035” that contribute toward an enabling of those roles;
- Third, validated reference scenarios that lead to the FOCUS roadmap proposal for “security research 2035.”

FOCUS results were obtained by expert workshops, online questionnaires, analyses of related foresight projects, and large horizon scanning. This was based on a methodology process, which was also part of the project's work. In total, more than 600 experts contributed to the results by scenario information crowd-sourcing and assessments, representing more than 20 countries. Experts were identified in horizon scanning, in scanning of related projects, and by using partners' lists of experts. Further experts were added based on project-related communication and turnout for project events. Participating experts represented EU bodies; NATO bodies and institutions; national regional and federal bodies; international bodies; industry; first responder and emergency management organisations and agencies; think tanks; universities; NGOs; and other sectors.

To integrate its foresight results, FOCUS designed and applied an “embedded scenario” method. This delineates options for future tracks and broadened concepts of security research within broader scenarios that involve EU roles for responding to transversal challenges (whose causes are external but whose effects are internal to the EU).

1.3 Reference scenario method

At the end of the scenario work, a reference scenario for each of the five “Big Themes” was derived. Those five reference scenarios for the planning of future security research in the overall 2035 time frame of the FOCUS project comprise the following:

- Alternative future concepts of the comprehensive approach and resulting role requirements for the EU – Reference scenario: “No Land is an Island” – A protected EU homeland with external responsibilities;
- Natural disasters and global environmental change – Reference scenario: “Policy Drives All in a

Have/Have-Not World” – security research on natural disasters and the global environment;

- Critical infrastructure and supply chain protection – Reference scenario: “Security as Societal Science” – Critical infrastructure and supply chain research driven by societal factors;
- The EU as a global actor based on the wider Petersberg tasks – Reference scenario: “Borderless Threats = Mission Creep” – The EU’s forced march toward a stronger Common Security and Defence Policy;
- The EU’s internal framework (and the emerging system of EU Homeland Security) – Reference scenario: “Inside Out” – Inward coherence and governance opens the door to external policy.

The five reference scenarios depict alternative futures for security research in 2035 that 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), described in the thematic scenarios for “EU 2035” security roles.

The basis for deriving the reference scenarios were the 24 thematic scenarios for “security research 2035” previously developed by FOCUS, plus a comprehensive online questionnaire for the assessment of those scenarios by external experts, stakeholders, and interested parties, as well as cross-referencing and plausibility-probing analytical work and further supporting analyses.

While any number of methodologies could have been applied to the five sub-sets of syllabus scenarios, the most logical approaches choices boiled down to two: 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. FOCUS rejected the former approach for its risk of skewing a scenario toward one extreme or the other (given the diversity of sub-scenarios within each “Big Theme”) or excluding relevant descriptors. Instead, FOCUS opted for the composite approach. The task then became one of devising a methodology to produce composite reference scenarios for each of the “Big Theme” scenario sub-sets.

The approach centred on the creation of a standard “scenario generator,” whereby the basic descriptive elements were extracted from each scenario within a given sub-set. The elements were then mapped against multiple relevant EU policies, working documents such as the final report of the European security research and Innovation Form (ESRIF), and/or known political stances of the EU and its 27 Member States. Then they were “filtered” or analyzed to determine whether the descriptive element remained valid for the 2035 time frame as projected through the assumptions that underpin those EU policy/stances.

Thus, each reference scenario generator allowed for a broad analysis of all key elements in all of the scenarios to be established per “Big Theme” against the EU’s wider policy environment. The filtering and selection task was enriched by parallel input from other FOCUS partners regarding their work on driver identification, expert questionnaires on selected “Big Theme” research, and other analysis. In total, reference scenario analysis included the following:

- Pre-validation (initial cross-reference) of sub-scenarios against each other and against general EU policy environment;
- Comprehensive assessment of the 24 thematic scenarios (EU roles as well as supporting security research) syllabus based on an online questionnaire;
- Identification of key drivers from the total set of FOCUS scenario drivers;
- Calibration of the draft scenarios with a compilation of future security research requirements resulting from alternative futures of the comprehensive approach.

Moreover, the reference scenarios were subjected to further analyses in order to support the FOCUS roadmap process. These analyses comprised the following:

- o Transversal analysis across the five reference scenarios concerning: external threats and their impact on EU security of citizens; the translation mechanisms these represent between external threats and their impact; and the identification of the impact of exogenous challenges on Member States as well as the limits to coherent EU roles – with the ultimate goal of identifying gaps in security research norms, standards, and procedures.
- o Assessment of differential impact of the “security research 2035” reference scenarios at national level.
- o Identification of requirements for future security research from other projects and comparison against the reference scenarios.

All FOCUS scenarios and related proof of concept information are available as wikis for further use on the IT-based Knowledge Platform that was developed in the project:

<http://www.focusproject.eu/web/focus/wiki/-/wiki/Main/FrontPage> .

2. Main steps and related results/usable output

The “Overview table of FOCUS steps and results/output” included in the attachments to this report provides an overview of FOCUS analytical, foresight, and integration steps, with main associated results and output. The table includes hyperlinks to publicly available project results documents and content.

The subsequent chapters describe results obtained from the major steps in the project.

2.1 Problem space descriptions and related future security research tracks

2.1.1 Introduction and transversal scenario drivers

FOCUS scenario foresight in its 2035 time frame was based on problem space descriptions per “Big Theme” that the project produced in the form of studies, taking into account the results of foresight and scenario work conducted in other European and international projects. In this context, the following seven

transversal scenario drivers for the evolution of the European civil security challenges policies (across FOCUS' five "Big Themes") were derived.

Based on the problem space descriptions and drivers, FOCUS then performed in-depth foresight processes. In the course of this, FOCUS at first identified future security research tracks. These were then reflected – along with broader foresight results from project work – in the development of the thematic scenarios for "security research 2035," as well as of the reference scenarios.

- Globalisation and international system change

Further effects of globalisation may lead to an international shift in relative wealth, revival of geopolitics, enhancement of global disorder, and a new form of multipolarity. This could produce a global redistribution of power, causing the EU to face increased friction when acting globally to provide security for its citizens. Increased friction means a transition from cooperation towards confrontation when making and enforcing decisions on the international level. Redistribution of power will also increase asymmetry (the relative difference between the capacities of states to influence international security affairs).

- Changing modes of governance

Governance – the evolving informal system, short of hard sanctions and enforcement, for conforming to international legal and social norms – may adopt new and different characteristics following diversification and different forms of power, new sources of power, and different ways of using power on the global scene. This includes geopolitics as control over territorial space, not only borders. Public-private cooperation in security theatres will also be an important factor.

- Changing values and norms

Partly related to evolving modes of governance, values, and norms also are relevant drivers of the internal political and social cohesion of the European Union. These will determine the sense of collectiveness and readiness of taking responsibility, and sharing the burdens of a global role. They will also strongly influence the EU's dedication to the protection of human rights and the fostering of human security on a global scale.

- Economic and social change

Economic and social change will determine alternatives for protecting societies and infrastructures. Relative economic power and the EU's prevailing perception of its own economic and social conditions will affect its will and ability to increase collective efforts and strengthen the concept of the EU's security as a whole. Economic and financial crises will make it difficult to counter threats in a comprehensive way. European demographics will influence public attitudes, the political will, and the political agency of the EU to act as a security provider.

- Technological change

This driver is multifaceted. It includes new technology-based capabilities of the Union and its Member

States, as well as new critical (inter-)dependencies – such as on information and communication technologies – and vulnerabilities. Vulnerabilities could, for example, emerge from cross-dependencies of critical infrastructure on information technology systems. Technological change will also have impact on energy dependency, increasing or decreasing it.

- Extent of common threat assessment

Future roles of the EU as a security provider will hinge upon the extent to which a common threat assessment can be reached on EU and national levels. This includes the evolution of current consensual threat drivers, which mainly are: CBNRe terrorism (chemical, biological, nuclear, radiological, and explosives); external political instability, poverty and resulting mass migration; cyber threats; and climate change, including its effect as a threat multiplier.

- Consistency and coherence of future security research

The thrust of the EU as a comprehensive security provider to its citizens will depend on the degree of consistency and coherence of security research at national and EU levels. Consistent security research accumulates knowledge across disciplines, sectors, and cases in order to timely identify most important gaps and needs for the further implementation of security strategies. Coherent security research is a cooperative intellectual effort at national and EU levels that contributes to the definition and implementation of a common European security agenda across different themes, funding lines, epistemic communities, and stakeholders.

2.1.2 Comprehensive approach

Challenges in the coming decades will be fraught with uncertainty, involving state and non-state actors who combine conventional and asymmetric methods. They will encompass space and cyberspace, and influence the concept of comprehensive security as well as operational ingredients of the comprehensive approach. Shaping the opinion of a network-enabled audience will be just as important as targeting the threat. Problems related to the proliferation of weapons of mass destruction will persist. Cyber threats will also proliferate, with possibilities for organising high-consequence attacks against European critical infrastructures. Likewise, non-state and hybrid actors will continue to seek the ability to stage major terrorist attacks on the territories of EU Member States as well.

A comprehensive approach aims at overarching solutions to problems, generating broad effects and based on the 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 entails the tackling of cross-cutting issues in home affairs, including civil protection. Reflecting the cross-border and cross-sector nature of current threats and challenges as well as the complexity of instruments and objectives along the internal–external continuum, a 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.

Future tracks of security research should include the following: EU cohesion, decision-making and, more

generally, governance; dependency on information and communication technology, and technology in general (address cascading breakdown of systems); new methodologies for collecting and integrating data from various different sources; decision-making tools based on joined-up situation analyses, including their use to secure public acceptance and support; advancement and integration of approaches to foresight, with special consideration of disruptors from normative (desired) end-states. Future tracks of security research should also lay emphasis on the implementation perspective, taking into account indicators for measuring the effectiveness of the comprehensive approach.

2.1.3 Natural disasters & global environmental change

Addressing natural hazards, with serious consequences on a regional level, FOCUS centres on major external threats to greater areas (outside and within the European Union) that may shape future roles of the EU as a comprehensive security provider: They can cause humanitarian crises of scales requiring a wide spectrum of responses, as they affect infrastructures and human environment. Moreover, interactions of different hazards, multi-hazards, technological hazards, and the fact that human activity can initiate or influence processes and events, will play an increasing role.

Future research therefore should act as a catalyst in the form of meta-projects integrating results from EU funded and other projects on natural hazards and their security aspects. However, this would require enhanced accessibility of previous studies and their results. Improved dissemination strategies will be required. Other topics could be anthropogenic (or “man-made”) natural disasters and multidisciplinary scenarios of maximum credible natural events. Those scenarios could contribute to identifying maximum possible damage from a combination of primary (destruction by shockwave), secondary (e.g. fires), and tertiary (e.g. supply chain damage, loss of production) effects for a given region, nation, or the EU as a whole. Moreover, future research should investigate drivers of change in individual behaviour in relation to climate change mitigation.

2.1.4 Critical infrastructure & supply chain protection

Critical infrastructure protection, including the cyber dimension, refers to preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. More specifically, critical infrastructure protection as defined by the EU is the ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction, as well as to protect human lives.

Over the past decade, the EU has taken substantial steps to formulate integrated policies designed to enhance the protection of European Critical Infrastructure (ECI) and reduce its vulnerability to a variety of threats, including terrorism, criminal activities, and natural disasters. The most significant advancement has been the introduction of the European Programme for Critical Infrastructure Protection (EPCIP). EPCIP embraces an all-hazards approach, covering natural disasters and intentional anthropogenic (or “man-made”) hazards. Effective protection will need binding international and global rules, since major infrastructures operate internationally or globally and threats can originate from any place in the world.

Policy developments call for support by well-focused EU-level research, which should include three main themes. First, there is the need to conduct detailed assessment on interdependencies in the European Critical Infrastructure system. Special attention should be paid on linkages between European Critical Infrastructure and infrastructure located in third countries. Second, future research should compile a comprehensive catalogue of critical supplies for the European economy and investigate factors that could disrupt supply of these materials to the EU in detail. Third, more research is needed to analyze how the new mandate of the Lisbon Treaty together with enhanced capabilities of the EU could change the EU's role in foreign politics, and more interestingly, how the EU could use its growing political power to secure its interests in third countries.

As far as the cyber dimension is concerned, future research should moreover address cyber attacks on commercial and state actor targets – and if dissuasion is possible and what are effective responses to such attacks – but also hacking and other actions from cyberactivist groups.

2.1.5 The EU as a global actor based on the wider Petersberg tasks

In view of the expansion of the EU's direct involvement in security affairs in recent years, this should lead to EU future endeavours that cut across the range of the Petersberg tasks. Any related concept of the EU as a global actor should be realistically based on the EU's posture in order to provide the most relevant package of concepts and capabilities to every particular case.

The 2008 implementation review of the European Security Strategy (2003) stressed that the Union disposed of an unmatched repertory of instruments and activities to foster human security and address underlying causes of insecurity and conflict. Based on this, the EU should contribute to renewing multilateralism at the global level. 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, including in security sectors; or civil society-related and cultural instruments, including media, social networks, etc.

Future concepts of a global security role for the EU will require even more than present ones that the Unions' security posture (strategic orientation plus capabilities) and its internal decision-making framework match. Future security research should address 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; and challenges that result from differentials in the EU's wider neighbourhood (population, age, employment, competence, etc.).

2.1.6 EU internal framework (and EU homeland security)

The evolution of the EU's internal structure will be driven both by external challenges and by internal

pressures to forge collective policies in order to maintain institutional coherence and thus deliver effective, consistent responses to major external challenges. Some of the EU's vulnerabilities result from the fact that European strategies do not always take into account the resources required for their implementation and do not fully consider organisational needs to effectuate awareness and increase resilience. Given the experience of several crises of different types in recent years, the EU internal framework is going to change further, with an emphasis on institutional qualities and European capabilities to provide comprehensive support to the European citizens in times of crisis.

While EU Member States agreed to introduce the concept of the security of the Union as a whole into the Lisbon Treaty, both the political and the public sector considerably vary across countries in their perceptions and concepts of security. The concept of security in the EU so far has been the resultant of Union-level initiatives and national repertoires of action. Member States continue to rest on different symbols of what they value and safeguard. There are different public and citizen security cultures, leading to nationally informed priorities. Divergences of such kind notwithstanding, the future concept of security as well as of security research can be expected to be informed by the European Security Model as outlined in the EU Internal Security Strategy. This includes addressing the causes of insecurity and not just its effects, with priorities on prevention across sectors (political, economic, social, etc.).

New tracks of security research comprise the need for the EU to support Member States in times of crisis, including for example possible increased roles of dual-use capabilities in home affairs. Another aspect is to identify most important research gaps and needs for the further implementation of EU security strategies. The role of the internet, in particular of the new social media such as Facebook, is a further relevant aspect that follows the need for differentiated analyses of such as emergence of networks combining factions, future strategies, and technologies to interfere with riot communication, future police capabilities, and oversight mechanisms.

2.2 Key technology aspects of the problem spaces

FOCUS foresight yielded insight in key technology aspects relating to the "EU 2035" as a comprehensive security provider to its citizens, as per the problem spaces laid out above. Key technology aspects were identified – per "Big Theme" – in the following two dimensions:

- Expected key security technologies in future EU security roles;
- Requirements for IT-based knowledge management in future EU security roles, based on exploration of use of the FOCUS IT-based Knowledge Platform and its potential for expansion beyond the immediate scope of the FOCUS project.

2.2.1 Expected key technologies in future EU security roles

2.2.1.1 Comprehensive approach

- Chemical and biological sensors; X-ray technology
- Imaging technologies
- Data fusion and decision support software
- Mobile broadband communication – developed possibilities to exchange information over long-distance in real time, with high quality and reliability
- Technology platforms and convertible technologies
- Multi-use platforms (civil, security, military, etc.)
- IT key platform technology
- Vulnerability and response capabilities simulation

2.2.1.2 Natural disasters and global environmental change

- Smart power grids
- Electromobility
- Decentralised power generators
- Uses of smartphones for individualised (or more individualised) emergency assistance
- Service robots

2.2.1.3 Critical infrastructure and supply chain protection

- Data protection technology
- IT security technology (relates both to improved conventional anti-virus technology and to new anti-cyber attack technology)

2.2.1.4 The EU as a global actor based on the wider Petersberg tasks

- Unmanned aerial vehicles
- Image processing equipment
- IT intelligence: web search instruments

2.2.1.5 EU internal framework (and EU homeland security)

- Technologies for collaborative e-government
- Technologies for inter-agency cooperation
- Cyber intelligence web technologies
- Space technologies

2.2.2 Requirements for IT-based knowledge management in future EU security roles

2.2.2.1 Comprehensive approach

- IT-based knowledge management platforms that allow for both strategic and mission scenario planning
- Use of IT-based knowledge management platforms for information interoperability and integrated situational pictures
- Providing meta-technology to integrate and comprehensively use data and information from different sources to allow for more informed and better decisions
- New technologies for collecting and integrating data from various different sources
- Syllabi of mechanisms of external threats on EU critical infrastructure, mainly related to information and communication technology (ICT) and cyber attacks
- Collection of definition of future operational requirements and technology development
- Platform technology for structured information exchange, e.g. inter-agency

2.2.2.2 Natural disasters and global environmental change

- Use of IT-based knowledge management platforms as part of a holistic educational system that increase societal sustainability and resilience: understanding, interdisciplinary, and strengthening intrinsic values such as cooperation and solidarity
- Advancing disaster forecast technologies and integrating information gained based on those technologies
- Use of IT-based knowledge management platforms to foster and integrate output from technology assessments and creative thinking
- Technology for structured exchange of information
- Knowledge management and knowledge integration
- Platform for crisis communication
- Platform to support crisis management (e.g. knowledge-based decision support)
- Platform for education and training of decision-makers and first responders

2.2.2.3 Critical infrastructure and supply chain protection

- Crowdsourced technology foresight and assessment
- Hosting of a dynamic model to describe interdependencies among critical infrastructures and supply chains
- Critical Infrastructure Warning Information Network
- Crowdsourcing of citizens' perception of infringements of their fundamental rights by increased security of infrastructures and supply chains
- Knowledge management and knowledge integration, including contribution to education of society on the vulnerabilities, on the consequences of failures, and on the way to behave in case of disaster
- Platform for crisis communication
- Platform to support crisis management (e.g. knowledge-based decision support), facilitating interoperability and collaboration between EU Member States

2.2.2.4 The EU as a global actor based on the wider Petersberg tasks

- Knowledge management and knowledge integration, in particular relating to comprehensive situational awareness; cooperative vulnerability assessment; and common operational picture process and integration of early-warning information
- Crowdsourcing of technology opportunities/possibilities vs. citizens' needs
- Platform for crisis communication
- Platform to support crisis management (e.g. knowledge-based decision support)
- Platform for education and training of decision-makers and first responders

2.2.2.5 EU internal framework (and EU homeland security)

- Knowledge management and information integration for situational awareness, in particular including information/results from use of new forecast technologies
- Knowledge/knowledge-management related challenges of deepening interdependence
- Structured exchange of information for inter-agency collaboration
- Crowdsourcing of technology opportunities/possibilities vs. citizens' needs
- Platform for support of crisis management (e.g. knowledge-based decision support)
- Platform for crisis communication
- Platform for education and training of decision-makers and first responders

2.3 Reference scenarios

2.3.1 Development and overview of the reference scenarios

Based on a broad plausibility probe and on online questionnaire work involving more than 100 experts, stakeholders and end-users from more than 20 countries from within and outside the EU, FOCUS developed the following reference scenarios. The FOCUS roadmap development towards “security research 2035” then built upon those reference scenarios.

The five reference scenarios for the planning of future security research in the overall 2035 time frame of the FOCUS project comprise the following:

- “No Land is an Island” – A protected EU homeland with external responsibilities;
- “Policy Drives All in a Have/Have-Not World” – security research on natural disasters and the global environment;
- “Security as Societal Science” – Critical infrastructure and supply chain research driven by societal factors;
- “Borderless Threats = Mission Creep” – The EU's forced march toward a stronger Common Security and

- “Inside Out” – Inward coherence and governance opens the door to external policy.

As explained above, these reference scenarios depict alternative futures for “security research” in the 2035 time frame which support the EU’s projected exogenous security roles described at the level of thematic scenarios.

The reference scenarios provide various insights into what future European security research may require. This includes respect for human and societal needs, citizens being the ultimate end-users of security research. The reference scenarios also assume that security missions of the “EU 2035” will increasingly stretch along the internal–external security continuum and that full integration of emergency management and civil protection within the scope of security research will be vital, along with its elevation to European level. Coordinated investment in preparedness is expected to play a major role here.

The two reference scenarios “Policy Drives All in a Have/Have-Not World” (security research on natural disasters and the global environment) and “No Land is an Island” (A protected EU homeland with external responsibilities) can be expected to have the highest impact at national level. Of the countries that have national security research programmes/strategies in place and were covered in the assessment, Austria, Germany, Norway, Sweden, and Spain would be most strongly affected by the reference scenarios, should they materialise. Materialisation of the scenarios would have strong overall impact on France, Italy, the Netherlands, or the UK. These countries could largely proceed with their current security research approaches and security strategies to meet the scenarios’ requirements.

While the reference scenarios have different loads on the drivers and a different thematic focus, the following cross-cutting scenario descriptors common to all reference scenarios were identified:

- Monitoring/detection/surveillance instruments for external threats;
- Comprehensive risk and vulnerability assessment;
- EU as a comprehensive security provider, including the approach to resilience of systems, infrastructures, and societies;
- EU legislative frameworks evolve toward more inter-institutional and international cooperation;
- Security research merges with emergency management and disaster research;
- EU role embraces coordination, data exchange, and early alert;
- EU’s security–safety continuum grows stronger;
- EU’s internal (homeland) security policy increases;

- Ethical research rises to the top of EU research agenda, with increasing focus on influence of societal factors on security strategies;
- Critical infrastructures and supply chains adapt to societal changes and security needs;
- Societal awareness increases via citizen education and risk communication;
- Advanced public-private partnerships for security technology development and implementation;
- Harmonised risk management for preparedness and response at EU and Member State level;
- Comprehensive risk assessment framework for critical infrastructures and supply chains;
- EU has new public funding mechanisms for technologies aimed at closing security gaps;
- security research is supporting policy and strategic studies for early warning purposes, with emphasis on CBRN mission scenarios.

This in the first place means the EU should look for ways in which technologies and capabilities can support a stronger comprehensive approach for common emerging and future security threats. FOCUS insights on cross-cutting aspects speak in favour of a future European security research system that better accommodates social sciences and humanities in order to propose ways to more strongly link civil security authorities to citizenry, and citizenry to technologies.

Among further conclusions for “security research 2035” drawn by FOCUS is that that future European security research should meet the challenge to develop a new concept of (civil) security from research, rather than deriving it from events, technologies, or existing policies. It should also clearly address the risk of an uneven distribution of security across European society, for example by using technologies that only add to the security of the wealthy, or by deploying security solutions that even may harm certain parts of society. At the same time, future research planning should more comprehensively address social media communications technologies for their ability to better connect policymakers and civil security end-users to public/civil society audiences, and to enable policymakers to communicate to the latter.

FOCUS scenario foresight took as its point of departure the project’s five “Big Themes” as described above, and while not necessarily intended to do so, the reference scenario process resulted in scenarios where each mainly represents one of those “Big Themes.”

2.3.2 Reference scenario summaries

2.3.2.1 “No Land is an Island” – A protected EU homeland with external responsibilities

In 2035, the EU and its Member States have developed a common “securitisation 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 to help Europe deal with security incidents. This collective policy-foundation determines which topics will fall under security research, whose results are fed into trans-disciplinary information and data architecture that is made accessible to a wide range of EU stakeholders involved in Europe's internal and external security domains.

The "securitisation model" approach has led to the definition of systematic "qualification profiles" regarding human resources and technical advances, which have been embedded into academic curricula. The goal is to shape future generations of security researchers and stakeholders within the context of the EU's comprehensive approach to internal and external security policy.

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 an integrated risk-management/all-hazard approach for coping with security threats to the Union's own territory. The EU's definition of security has expanded to establish many connections to safety as well. This complicates the capabilities required but ensures a more complete approach to the EU's security-of-the-citizen imperative, while linking to relevant industry strategies and programmes.

Internally, the EU has substantially expanded its early-warning capabilities and rapid-alert systems regarding civil threats. It has also built on national-owned civil protection modules of disaster response capabilities with its own layer of EU-owned or leased capabilities to supplement gaps across the Union. Resilience involving cross-border critical infrastructure, however, remains weak for lack of strong EU regulation of the sector.

Externally, the EU's policy building-blocks are more restricted. Its comprehensive approach in this domain is basically one of coordinating autonomous actors who share information and pool resources due to domestic budgetary restrictions. Nonetheless, the securitisation model generates requirements for each of the EU's approved roles as comprehensive security provider, with identified gaps in capabilities addressed through targeted research efforts.

While the EU also now owns some CSDP (Common Security and Defence Policy) assets, most still belong to the Member States, though their mutual supply dependency has increased due to tighter pooling and sharing of assets compared to 2009, when the idea was first launched. The EU's intra-governmental "Athena Fund" for external missions has expanded beyond strict funding of only common Headquarters costs to include certain deployment and other operational costs.

For external application, security research supports the development of technical capabilities to link the autonomous actors of EU missions together such as data-exchange systems and situational awareness. It also supports skills development and training to enable the EU's strategic and operational missions to cover all aspects (socio-economic, environmental, societal, political, etc.) of the crisis management cycle, from mitigation and preparedness to response, recovery, and reconstruction.

Internally, the securitisation model has led security research to crystallise around half a dozen broad themes. One embraces cost-benefit analysis and the identification of vulnerabilities of centralised versus decentralised economic and administrative systems. Another one targets assessment of technologies for

their ecological impact which, however, carries the risk of slowing the technologies' implementation.

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. Hence, it is difficult to reach case-by-case consensus on their use. Moreover, major security research themes stress supply chain security (including critical infrastructures in banking, financial and insurance networks); mission scenarios arising from chemical, biological, radiological, and nuclear threats; and public health security issues linked to risky products, procedures and services. Given that cybercrime is a global phenomenon causing significant damage to the EU's internal market in 2035, a research track is dedicated to the cyber dimension of security.

A final overarching security research theme is data integration, particularly the extent to which standards-based information can be distributed across multiple public and private-sector organisations and their sub-units. This is critical to the management of communications, improved operational coordination as well as integrated planning and decision-making across the EU, its Member States, industry, societal, and first-responder groups. However, public and private sectors alike have understood that achieving an optimal level of data integration involves a trade-off: higher coordination means a decrease in local flexibility – and possibly effectiveness. This demands a combined bottom-up approach that connects academic disciplines involved in broad foresight to various stakeholders within and outside the EU, with rigorous vetting of the compliance of security research activities and projects with the EU's ethical and data privacy rules.

2.3.2.2 “Policy Drives All in a Have/Have-Not World” – security research on natural disasters and the global environment

By 2035, there is growing awareness across decisions-makers in the EU that competing national and regional policies beyond their borders are producing an increasingly fragmented world, split into tiny privileged elites versus the teeming masses of “have-nots.” The rapidly evolving risk for everyone is a disastrous collapse of society and civilisation.

The EU wants realignment toward a consensual international policy designed to confront this divergence. But the regions retreat further into their own parochial agendas, where power derives from political groupings at the expense of society at large, democracy, and the environment. A central strand in the EU's security research programme is to develop internal and external security mitigation/adaptation strategies needed for a world split into haves and have-nots.

A parallel research strand aims to push back against this externality by focusing on ethics, individual freedom, and rights to further promote the EU's democratic structures, thus offering a role model to the outside world. The goal is to counter the threats posed to the global environment caused by competing regional policies. This calls for better communication and dissemination techniques to broaden the EU public's understanding of the regulatory and policy tools needed to mitigate those regions' deleterious policies.

Society is under pressure of rapid global environmental change. Research urgently needs to find ways to

combine prevalent short-term solutions to imminent problems with effective long-term measures. Inside the EU a certain degree of sustainable development technologies in 2035 has been taken up by the markets. Even this modest achievement gives the EU a leading role in the research and application of renewable energies and recycling technologies, where a huge international market has opened in response to costly fossil fuels.

At the same time, Europe's recycling has helped reduce its dependency on raw material imports such as copper and rare earths. The nuclear industry's rocketing safety and security costs, together with several severe accidents, are pushing the sector to extinction. Security research includes analysis of cheap, safe, and rapid techniques for dismantling the sector's infrastructure and minimising nuclear waste-related risks. Although EU policymakers in 2035 know that Europe's centralised electricity power grid is a main source of vulnerability to attack, decentralisation and localisation of energy production is not achievable, however, since it is opposed by the grid's large corporations that still own and control most of the infrastructure.

The EU in 2035 also wants better forecasting of natural disasters, a goal shared and co-funded by industry since better modelling would help reduce the overall cost of an event's impact. The systems aim to target the drivers of natural disasters and refine long-term forecasts about the planet's ecological limits. This "greener" research footing calls for evaluating the compatibility of technologies, trade regulations and international treaties with the global environment, as well as developing alternative fiscal systems that shift tax bases away from labour to resource use and waste.

Complementary EU policy in 2035 favours natural disaster resiliency linked to re-creating natural river beds and mixed forests to combat erosion and promote bio-diversity. This leads to a new EU land-classification system that supports organic farming based on old seeds and locally adapted, highly resilient non-GMO (Genetically Modified Organism) cultivars.

Despite its green efforts, new climate-change related diseases are on the rise in the EU. Combined with Europe's increase in life expectancy, these factors lead to huge investments in gerontology, while research examines how shifting habitats will generate new epidemiological threats, such as vector-transmitted diseases.

2.3.2.3 "Security as Societal Science" – Critical infrastructure and supply chain research driven by societal factors

In 2035, security management has become a risk-driven process. Collaboration between international organisations, Member States, EU bodies, civil society organisations and the private sector via security data compilation, crowd sourcing, and information sharing has led to the establishment of a harmonised risk management approach at EU and Member States' level. This covers both preparedness and response.

The EU 2035 faces strong demands for critical infrastructure by politics, industry, and society: Critical infrastructures and supply chains are desired to be designed adaptable to social change and evolving citizens' security needs and resilient to negative effects of interdependencies within Europe and with

critical infrastructures in third countries. Broad-scale public private partnerships are put in place for development and implementation of critical infrastructures, and supporting research, to meet these demands and close security gaps. Critical infrastructures are also desired and required to have a harmonised all-hazard driven security management approach, covering the full crisis management cycle and societal consequences of breakdown.

The EU recognises the high degree of interconnectivity and interdependency with third-country infrastructures (especially regarding energy, raw materials, and food supply chains). It thus seeks a legislative framework that supports inter-institutional and international coordination of critical infrastructure and supply chain protection. It also seeks the adaptability of critical infrastructures and supply chains to societal factors changes, evolving security conditions, and the gaps that emerge from these. Policy focuses on developing rapid response mechanisms to manage social stress caused by supply chain disruptions.

A significant strand of security research has developed into a social science discipline addressing the influence of societal factors on security strategies. The public perception of security technologies and their benefits for critical infrastructure and supply chain protection still varies greatly across the Member States. This calls for increasing societal awareness through risk communication and citizen education, particularly in view of the potential loss of public trust in institutions and agencies at national and European level should critical infrastructures of supply lines fail.

A comprehensive approach to creating resilience of infrastructures and societies is needed, and new public funding mechanisms for technologies to close security gaps are under review. However, much of this responsibility in 2035 has shifted to the private sector and public-private partnerships. Governments rely heavily on the latter for analysis of supply chain and their interdependencies, management, and resilience. Policy objectives include a comprehensive cataloguing of critical supplies for the European economy, along with the factors that could disrupt the supply of these materials to the EU.

Though technologies in 2035 have seen improvements and new options for critical infrastructure and supply chain protection, the EU's decision-making process for emergencies is still too cumbersome. Better technological solutions in the form of visualisation tools are needed to support the monitoring of large-scale interdependencies between critical infrastructures and supply chain networks.

To minimise the impact of security incidents on these infrastructures, and to mitigate long-term social, political and economic impacts of breakdown and disruption, the EU and its Member States have agreed to a mutual support system based on openness and cooperation. Security research thus includes organisational studies about incident awareness and the most optimal managerial and decision-making structures. Experience has shown that data integration can also augment related costs and create security gaps by increasing the size and complexity of the design required. Security research assesses the pros and cons of various levels of data integration from the point of view of cost and trade-off between complexity and size. Indeed, research also focuses on the interdependencies lying along the EU's internal-external security continuum. This calls for scenario-related cross-border simulations of incidents involving supranational supply chain networks, with advanced risk assessment methodologies that reflect unexpected changes such as new threats or breakdowns of interconnected infrastructures – an effort that

knits together a broad range of disciplines, from physical and logistical security to threats to human safety and the environment.

2.3.2.4 “Borderless Threats = Mission Creep” – The EU’s forced march toward a stronger Common Security and Defence Policy

In 2035, 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. Continuous cooperative vulnerability assessments involving as many countries as possible have become a priority. This requires technology assessment expertise, simulation capabilities, legal and economic innovations, as well as capability developments running along the defence–security continuum.

In its 2035 operational environment, the EU has seen an expansion of simulation capabilities, in particular in the functions of high-tech monitoring systems such as Copernicus and Galileo for strengthening EU action across its crisis management cycle. A strong transatlantic framework of homeland cooperation has emerged, though it is geared towards joint pragmatic/operational action, but not necessarily towards joint technology development. Internally, there is a risk of the EU having developed over-sophisticated capabilities in response to a permanent structured cooperation in security-defence matters agreed by a core of self-selected Member States.

Elsewhere, political pressure across all the Member States has led to a strong focus on collectively managing maritime crises in a highly competitive environment. This trend grew steadily from earlier in the century as the EU’s global reach expanded via the necessary translation of the Common Security and Defence Policy (CSDP) into practice in order to confront external threats and challenges. The EU thus fosters the exploitation of dual-use technologies within a “smart defence” context. This approach is reinforced by the EU Member States’ mutual dependence and vulnerability of maritime security in 2035.

At the same time, political pressure has led to a parallel focus on non-technological security research and development in areas such as macro-economic financial instruments or EU industrial strategies. This calls for cost effective and comprehensive European solutions to support them, which however sees systemic resiliency tending to get priority over resilience of the citizen per se.

Meanwhile, certain security threats such as those emanating from the proliferation of CBRN (chemical, biological, radiological, nuclear) materials or failed states continue to be evaluated largely in a nationalist context. An exception is the threat of supply chain disruptions and how to manage them. There is an EU 2035 consensus across the Member States to prevent and prepare for disruptions in technological terms. This prompts significant EU research focused on the challenge, which includes strategic studies into early warning capabilities and to support CSDP decisions.

2.3.2.5 “Inside Out” – Inward coherence and governance opens the door to external policy

By 2035, the EU has become the governing authority of scientific and technological innovations related to

security of the citizen. A major policy imperative in 2035 has seen capability development lead to a convergence of research in the fields of civil security, policing needs, emergency response, and disaster management. This convergence has opened the way to linking the EU's internal decision-making structures and processes to its external strategic environment. Security research contributes to meeting related technology needs such as collaborative technologies for interagency work and intelligence sharing.

Progressive standards and codes of conduct are critical to enabling the EU to implement responsible technology governance. Citizens play a growing role in decision-making processes and are anxious that their rights and liberties, as well as foundations for living, are protected, while the EU expanded its internal framework into a homeland security system. Citizens want a role for the EU as a security actor – within and beyond the Union – but checked and closely overseen by the European Parliament and other mechanisms.

Climate change is indisputably accepted by EU 2035 policymakers as a limiting factor on key resources. One result is that also for this reason, national and EU decision-makers consistently focus on public perceptions of citizens' security needs. Security research among other things contributes new social media-based technologies for knowledge management and information integration.

Multidisciplinary mapping of fundamental rights enforcement and the acceptability of security technologies and interventions have become paramount across the EU Member States. Security research thus comprises a technology track and an institutional one that covers organisational analyses and critical studies linked to the EU's internal functioning regarding its security sector. Main research themes are based on promoting public-private partnerships and relate to commonly perceived strategic challenges of threats such as remote sensing, communications, mobility, critical dependencies, cyber attacks, CBRN (chemical, biological, radiological, nuclear), or climate change-related incidents, with a focus on development of capabilities for comprehensive use – together with advancing standards and codes of conduct for mainstreaming responsible technology governance.

Parallel to this development, organisational studies linking threats and risk assessments to decision-making have become valuable tools in 2035 for national and EU decision-makers. These focus on ever-growing strategic threats that can originate as easily beyond the EU as within it. Above all, however, a more efficient and effective EU internal framework is the first priority of research and policy. Security research therefore essentially includes development and improvement of educational measures enabling all-of-community approaches. It further includes critical studies of institutional qualities and European capabilities to provide comprehensive support to the European citizens in times of crisis, involving increased acceptable and accepted use of technologies.

2.4 The coming of societal security: Cross discipline/transversal aspects

FOCUS foresight results and horizon scanning affirm that “security” – all the more in its future shape and character – is a collective good that in the first place relates to citizens and society. Without public acceptance and inclusion of citizens in the creation of security and in the “production” of solutions to security problems, those solutions will be considerably limited in their effectiveness. This includes results from security research projects and their implementation.

FOCUS expects that future security research will become a part of the equation of security policy, and as such become a societal enterprise. A comprehensive approach to security research and to security in the EU therefore needs to consider and address citizens in an inclusive way, not only treating them as the ultimate end-users of security research. Rather, security research should focus on solving needs of citizens, not only on the impacts of security interventions. Citizens' perspectives should be integrated into the research process and into the programming of security research.

This is ever more important since it can be expected that technological innovation and further spread of networked structures will create new vulnerabilities, which will require increased societal awareness and resilience. Technology not only can contribute to security or by itself create new vulnerabilities. It also has the potential to change human behaviour and to drive the evolution of security cultures. Citizens' fear of being controlled by technology can change their behaviour as well as new opportunities for community activities, such as crowdsourcing of information about hazards and disasters to support mitigation, preparedness, response, and recovery. As those examples indicate, it can be expected that future development and application of technology will not by themselves create security or vulnerability. Rather, they will accentuate existing trends, processes, and repertoires of action that are socially rooted.

Social networks will play an ever growing important role in information dissemination, opinion mining, and public decision making. The unstructured and informal nature of social networks is a challenge for state authorities, which traditionally operate in a linear, top-down manner. This clash of cultures requires new procedures and training schemes for civil servants, officials, and volunteers.

Considering aspects like those, it becomes clear that there is more than the societal dimension of security: the societal creation of security.

There are no effective technological solutions without acceptance and public participation. With internal and external security becoming less and less separable in a variety of sectors, citizens will have to be better involved in security processes. At the same time, the further development of Europe's civil security cannot be conceived without technology, and technology will contribute to increase societal resilience. However, new technology can also decrease resilience as criminals and terrorists exploit it, which becomes most obvious in the cyber dimension. The coming of societal security will bring new challenges for industry and require improved and new products.

Drawing a conclusion from the above, not only a comprehensive approach that unifies efforts will be needed in the future, but also a holistic approach that comprises technology, society, culture, and change. As an all-of-society enterprise, future security research will require planning beyond traditional end-user satisfaction to anticipate societal requirements and stimulate future demand, thus contributing to the setting of requirements instead of just meeting existing end-user requirements.

Security does play a role in a variety of discourses, but it remains a vague term that is under constant change. Security research needs to increasingly include perspectives from the humanities and social sciences to provide practical criticism of the evolution of the concept of security in the EU and its impact on citizens and society. Security research should provide a better connection of the disciplines involved. It

should establish networked expertise for rapid decision support for end-users. In this context, security research should analyze citizens' security needs. It should also contribute to the continuous evaluation of national and European civil security strategies from both a scientific and a societal security point of view.

The reference scenario analysis also yielded main expected ethics aspects, including the following:

- Need of development of technology for privacy and trusted data by design along with security-enhancing technology;
- Assessment of security technology opportunities/possibilities vs. citizens' needs;
- Creation of different levels of security in society;
- Ethics of security economics (e.g. unintended consequences of "smart" and effects-based approaches);
- Increasing infrastructure for capturing, storing, linking, merging, processing, and visualising very large social media datasets with implications for fundamental citizens' rights, freedom of expression, and data privacy issues;
- Major consideration of non-technological issues such as trust and resilience;
- Risk of developing over-sophisticated technology that does not respond well to security gaps and/or citizens' needs;
- Risk of departure from normal liberal democratic standards (such as protection of liberties, separation of powers, and endorsement of checks and balances), for example in measures to drive/compel social and individual change of behaviour to mitigate climate change, or limit cyber vulnerability;
- Possible divergence between ethical security research and socially acceptable research: There can be a social consensus in favour of security measures that violate human rights, and security research that supports those measures;
- Need to provide norms and standards beyond security technology frameworks.

To better address those aspects in the future, FOCUS proposed ethics guidelines for security research, at the level of additional ethical review options for project proposals and in the progress of projects. This is part of the FOCUS roadmap proposal for "security research 2035" and the project's "Conclusions for 'security research 2035'," as summarised in the subsequent chapter.

2.5 FOCUS conclusions for "security research 2035"

With its emphasis on foresight (not prediction) and the transversal, ethical, and broader societal implications of its scenarios, the FOCUS project points to the emerging "Horizon 2020" programme by

supporting security research planning activities. However, the time frame of the FOCUS project is 2035, thus reaching beyond “Horizon 2020.” Consequently, FOCUS is not dedicated towards “Horizon 2020” itself but to longer-term planning for security research that supports the anticipated future roles of the EU as a security provider.

Scenario foresight results indicate that there may be sectoral confinements of the comprehensive approach by 2035, depending on the evolution of challenges. It may be that the concept of comprehensiveness guiding the “EU 2035” as a security actor will be centred on sectors such as critical infrastructure protection or public health, with multidisciplinary security research reduced to such sectors. A major conclusion therefore is that future European security research in the 2035 time frame should be geared to the creation of a suitable concept of comprehensive security, thus leading to the security of individual Member States and the Union as a whole. Future security research should 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.

FOCUS has shown that the planning of “security research 2035” will be driven by a variety of factors that apply across different themes and scenarios identified in the project. The top-10 drivers include:

1. Comprehensive (societal, economic, and institutional) resilience to crises and disasters;
2. Science and technology innovation;
3. Practical strength of the “European Security Model,” as advocated in the EU Internal Security Strategy (2010): addressing the causes of insecurity and not just the effects; prioritising prevention and anticipation, and involving all sectors with a role to play in public protection;
4. Asymmetry of capabilities of Member States, the EU, and adversaries – including regionalisation vs. globalisation of security;
5. Convergence or divergence of security cultures;
6. Extent of information and intelligence sharing, and early warning capabilities – including policies for information exchange;
7. Decision-making tools based on joined-up situation analyses, including their use to secure public acceptance and support;
8. Changing national security capacities and levels of asymmetry (relative difference between the capacity of nations to influence security affairs);
9. Whole of community approach based on technological facilitation and empowerment;
10. Extent of dependency on technology, as well as of critical (inter)dependencies between technologies.

Giving those multiple forces that are expected to shape the path towards “security research 2035,” the thrust of the EU as a comprehensive security provider to its citizens will depend on the degree consistency and coherence of security research at national and European levels.

- Consistent security research accumulates knowledge across disciplines, sectors, and cases, in order to timely identify most important gaps and needs for the further implementation of security strategies.
- Coherent security research is a cooperative intellectual effort at national and European levels to contribute to the definition and implementation of a common European security agenda across different themes, funding lines, epistemic communities, and stakeholders.

External challenges to the security of the EU in the coming decades will be fraught with uncertainty, involving state and non-state actors that combine conventional and asymmetric methods. These challenges will encompass physical space, cyberspace, and natural resources. High-intensity cyber threats attack against European critical infrastructures could easily generate a cascading effect on other infrastructures, with devastating consequences for society. While problems with the proliferation of weapons of mass destruction will persist, they may be superseded by threats from intelligent, unmanned devices designed for warfare and industrial espionage. These trends will increase conflict between global security and personal security, and the definition of the limits between privacy and public information.

In the light of these multiple challenges, security research should essentially include research into societal security. Among other goals, the results should provide advice to authorities for making the appropriate trade-offs between security and other valued societal objectives, while bearing in mind the deepening and widening of European integration and possible future Europeanisation of security-relevant policies. Relations between EU security strategies and its long-term visions such as the Digital Agenda will also have to be addressed.

Future security research should help identify and address – and not just note and implement – security-related challenges and requirements in both technological and non-technological aspects. In this vein, the planning of future security research, as supported by the FOCUS project, should consider which factors will drive evolution of the concept of security in the 2035 time frame.

FOCUS foresight yielded the following ranked top-10 drivers for determining what “security” might mean in a future “EU 2035,” with the factors of resources and resilience being the two most important groups of drivers:

1. Crises resulting from scarcity of resources (e.g. energy-caused stress and, most importantly, increasing scarcity of conventional oil; dependencies on supply chains);
2. Societal resilience and preparedness: Certain risks cannot be catered to or avoided, and societies must prepare for shocks and have the ability to recover;
3. Changing borderlines between internal and external security, including the extent of relations with the world’s leading countries;

4. Technological change, including new technologies that drive or change security needs;
5. Mass migration flows, e.g. due to economic disparity, global conflicts, natural disasters, and climate change;
6. International conflicts that involve cyber-techniques and/or competition for energy and other scarce resources;
7. Diffusion of power within and among nation-states, marked by the rise of densely populated and economically powerful China and India, as well as the increased importance of energy-rich states and regions;
8. Dependency on information and communication technology, and technology in general (with a focus on a cascading breakdown of connected systems);
9. Demographic shifts with pressure on resources;
10. Increased reliance on critical infrastructures which are vulnerable, have little spare capacity, operate at the edges of performance and loads, and are critically dependent on other infrastructures.

The instruments in support of the EU's global roles may include stronger justice and law enforcement capabilities; improved EU intelligence and early warning capabilities; financial instruments for influencing economic developments on a global scale; good governance and institution building in security sectors; or civil society-related and cultural instruments, including media, social networks, etc. Future security research should contribute to and build on those instruments. For an effective European homeland security system to emerge, future security research should address organisational issues such as integration of national and international agencies.

Future security research should also increasingly consider the societal impact of comprehensiveness. This will mean bringing together and applying various disciplines. It should aim to mainstream terminology to improve linguistic interoperability between different communities of practice and of knowledge, provide a better connection of the disciplines involved, establish networked expertise to provide rapid decision support for end-users, and contribute to continuous evaluation of strategies of national and European civil security strategies. Moreover, future security research should essentially include research into societal security. For example, it should involve a track dedicated to quick response mechanisms for managing social stress resulting from interruption of supplies.

Future security research should overall emphasise and help promote the principle of societal/citizen ownership (which views citizens as the final/ultimate end-users). This will be of increasing importance for the ethical and factual acceptability by the public of its results. At the same time, future security research should clearly address the risks of creating an uneven distribution of security across society, for example by technologies that only add to the security of the wealthy or security solutions that may even harm certain parts of society.

Future security research tracks should finally include critical thinking (as opposed to an approach based on predominant end-user requirements) about past and existing concepts and how they may develop in the future. Also, mechanisms such as public consultation should be explored to increase transparency about the aims of security research and the potential use of technologies developed under its aegis.

Finally, future security research should contribute to establish institutionalised relations between those actors involved in realising societal security; and it should make a specific contribution to the knowledge pool of the implementing organisation(s) and to the building of sustainable excellence of research and expertise, effective beyond project lifetime.

FOCUS overall results reinforce the following set of criteria for good security research, conscious of its broader societal impact. Security research should:


- Be based on the understanding that security mainly refers to people and society, and that technical solutions are not effective without the acceptance and participation of the public.
- Include advice to authorities to make appropriate trade-offs between security and other valued societal objectives in the context of the deepening and widening of European integration and possible future Europeanisation of security relevant policies.
- Consider significant social, cultural, ethical, legal, and political aspects of security from the very beginning of the research and development activities, that is, not only in the implementation perspective and in terms of public acceptance and ascribed legitimacy of its results and products.
- Promote critical discussion of fundamental concepts – whether established or innovative – and their societal impact.
- Involve a track dedicated to quick response mechanisms for managing social stress resulting from interruption of supplies.
- Recognise that its technological innovations may also cause new societal vulnerabilities or create different levels of security in society.
- Strongly consider that new technological environments should support the self-help capacity of the citizens, and that new technologies can change the structure and perception of crises and their management.
- Strengthen – especially against the backdrop of “resilience” – a whole-of-community and ownership approach to security. As such, security research should act as a socialisation vector that builds resilience clusters that wherever possible comprise technology/capability, first responders, and ordinary citizens.
- Help establish institutionalised relations between those actors involved in realising societal security.

- Make a specific contribution to the knowledge pool of the implementing organisation(s) and to building sustainable excellence of research and expertise which is operational and effective beyond a project's lifetime.

2.6 FOCUS roadmap proposal for “security research 2035”

The FOCUS roadmap reflects the project's main conclusions for “security research 2035,” as led by the project's idea of making a contribution to a trans-disciplinary security research paradigm. The FOCUS roadmap proposal for the planning of “security research 2035” is geared towards implementation of anticipated research requirements as they arise from the FOCUS reference scenarios, as well as from analysis of cross-cutting (cross-scenario) aspects and transversal issues that are scenario-independent. The roadmap moreover integrates FOCUS results such as the curriculum matrix, and provides a knowledge landscape for the systematic selection of FOCUS content and results per roadmap track. A public “light” version of the roadmap is available on the IT-based Knowledge Platform.

2.7 FOCUS website

This FOCUS website (<http://www.focusproject.eu> ) is – and will remain after the project – the single entry point to FOCUS information (such as objectives, method, related projects, etc.) and products (such as deliverables, publications, and the IT-based Knowledge Platform).

2.8 FOCUS IT-based Knowledge Platform for support of foresight scenario-based planning for security research

2.8.1 Overview and knowledge landscape of the Platform

FOCUS developed an IT-based Knowledge Platform, populated with studies done in the project and with tools developed or collected by the project, as well as with scenario information based on FOCUS foresight results. The immediate purpose of the Platform is to support planning of security research that is based on futuristic scenarios. Moreover, possible uses of the Platform beyond the immediate purpose of the FOCUS project were explored, with some implemented in the final version of the roadmap, such as planning for mission scenarios.

The IT-based Knowledge Platform is the central entry point/landing page and knowledge management site for IT-related tools and supporting environments for scenario foresight, following the FOCUS project methodology. The main focus of the IT-based Knowledge Platform is to establish a structure where tools and scenario foresight instruments and results can be integrated and made publicly accessible. With the exception of some confidential content, the Platform is accessible without user/password restrictions. For validation purposes and in compliance with data protection regulations as well as the FOCUS information security strategy, a token-based system is in place for scenario foresight questionnaires implemented on the Platform, with hyperlinks to related online content. The document “FOCUS IT Platform main

workbench” as included in the attachments to this report provides an overview of the knowledge landscape of the Platform.

2.8.2 Technological basis and development of the Platform

The IT-based Knowledge Platform was developed as a part of FOCUS research work in order to explicate scenario foresight findings in a sustainable, IT-supported way. The goal was to externalise expert knowledge to such an extent that it can be consumed and used by others. The corresponding objective was to create a knowledge platform that supports not only collaboration between subject-matter experts but also hosts and makes selectable the knowledge created within FOCUS in such a way that other experts, projects, and end-users can follow the path provided by FOCUS in the future in their own scenario foresight and research (planning) work

To achieve this, well-established knowledge management procedures were applied, building on the model-based knowledge management approach. This approach uses knowledge management and knowledge working environments, and it further improves the use of knowledge management models to support web platforms.

The IT-based Knowledge Platform defines a so-called knowledge execution environment. For knowledge management purposes, the modelling tool PROMOTE® was used and further improved. For the knowledge execution platform, LIFERAY technology was used as basis technology and enriched with model-driven execution components from PROMOTE®. This technical development and deployment was performed in parallel to the various FOCUS scenario foresight processes and the collection of knowledge from subject-matter experts. Knowledge extraction was achieved via typical workshop and knowledge harvesting techniques in order to collect and externalise knowledge. This work was applied in each of the five domains (or “Big Themes”) of FOCUS and – rooted in the methodological baseline described in Deliverable 2.1 – extended to fully implement a process-oriented knowledge management approach.

The main entry point is the so-called Workbench that provides different sections, listing various tools, resources, and products.

There are several sections on the Platform representing the roadmap, the knowledge products for each individual “Big Theme,” as well as cross-theme content such as the European Security Glossary, scenario Wikis, scenario syllabus Wikis, or supporting material.

2.8.3 Wikis

Implemented on IT-based Knowledge Platform, FOCUS wikis make scenario-related results and information available in various ways, including:

- Five “Big Themes” – providing the basis for FOCUS scenario foresight, and related knowledge space.

- Scenarios for security roles of the “EU 2035” – with futuristic mission scenarios for the EU as a security provider in the world of 2035 scenarios (alternative futures) for "security research 2035" to support "EU 2035" security roles.
- Scenarios for “security research 2035” – to support those roles.
- FOCUS reference scenarios – the basis for the FOCUS roadmap for the planning of future EU security research.
- FOCUS foresight methods wiki – apart from providing basic information, aims to make experience from the FOCUS project available for subsequent projects as well as interested experts and researchers who intend to conduct scenario foresight. The wiki also includes a foresight tools repertory compiled by FOCUS.
- European Security (Research) Glossary (ESG) –currently comprises more than 500 articles. It is a living document that will evolve beyond the lifetime of the FOCUS project. It explains acronyms and terms (with references) relevant for EU security and for the planning of security research in a 2035 time frame, as covered by the FOCUS project. Glossary content has been compiled from FOCUS deliverables and documents as well as supporting desk research. FOCUS created this basic glossary on security research to promote a common understanding on the subject for use by the public, authorities, researchers, and practitioners.

Wiki implementation of results and information is intended to maintain the FOCUS momentum beyond the project’s lifetime, facilitate take-up by stakeholders and other projects, and provide a dynamic content structure that can be further developed.

2.8.4 Process stepper

As an essential analytical part of the FOCUS IT-based Knowledge Platform, the process stepper (see illustration “FOCUS scenario foresight process stepper“ in the attachments to this report) for scenario foresight covers the phases of “scoping,” “modelling,” “threat analysis and filtering,” and “synthesis.” To walk through the FOCUS scenario foresight knowledge path per “Big Theme,” the user can select one of the phases to access the appropriate process stepper. Each process stepper supports the user by guiding you through its knowledge steps and offers additional supporting information for performing scenario foresight based on the FOCUS method.

2.8.5 Scenario foresight tool repository

A repertory of scenario foresight methods and tools was established for use in the development of the FOCUS scenarios, of the reference scenarios, and for use beyond the project. This repertory contains tools that were developed by FOCUS (process stepper, scenario foresight questionnaire repository, European security research Glossary (ESG), document repository, etc.), as well as tools publicly available

on the internet that were identified and used by FOCUS

(<http://www.focusproject.eu/web/focus/wiki/-/wiki/METHODS/FOCUS+tool+repertory> ).

Potential Impact:

1 FOCUS output structure and products for follow on use


FOCUS foreground is generally planned to be exploited by publications in relevant journals, edited volumes, etc. This is for different purposes such as expert and citizen education; policy planning; advancement of academic state of the art; etc.

In general, FOCUS' university partners intend to use the project's curriculum-related results to expand their existing study programmes or launch new ones. Partners expect to stimulate interest from new areas of potential students via course offerings in "new security studies."

It is also expected that FOCUS results will evoke interest on the side of the EU or national agencies to consider them in their planning and implementation activities related to security research in the post-FP7 era.

The figure "FOCUS output structure" as included in the attachments to this report illustrates the FOCUS project's output landscape.

The figure "FOCUS usable output" as included in the attachments to this report summarises FOCUS products for use, including beyond the lifetime of the project.

In particular, the FOCUS website, the IT-based Knowledge Platform and its roadmap for planning of "security research 2035," scenario wikis, the European Security (Research) glossary, etc. will remain available on <http://www.focusproject.eu> . At the same time, several follow-on actions are planned.

The dissemination, follow-on use and exploitation strategy of FOCUS rests on this continued availability of content, tools, and functionality of the project's website and IT-based Knowledge Platform. It is planned to raise commercial interest in using the IT Platform technology and provided a scenario foresight questionnaire repository with a questionnaire construction tool.

Main goals of the FOCUS project included the dissemination of the obtained knowledge in order to contribute analytical foundations for security research planning for Horizon 2020 and beyond. This will lead to the development of a shared, harmonised understanding of new tracks in security research, and the comprehensive approach with a focus on exogenous challenges.

To sum up, FOCUS in particular has the following potential for impact:

- To disseminate the large quantity of knowledge and expertise that will gradually become available in the course of the FOCUS project;
- To interact with envisaged end-users of the FOCUS project to ensure that the results produce maximal societal impact and visibility;


- To take into account the different perspectives of these end-users (supranational, national and local authorities, and professionals working in the field);
- To take social responsibility in any case that information may come up during the course of the FOCUS programme that may be useful or needed to be shared with authorities;
- To integrate FOCUS results in academic training materials and sustainable business models.


2 Conferences, workshops, and fairs

The consortium took full advantage of existing scientific community and stakeholder infrastructure (such as conferences, periodicals, and publication platforms) for communication and dissemination of security foresight-related project results. Several FOCUS partners are associated with one or more of those platforms. FOCUS participants moreover presented project results on more than 25 external conferences in more than 15 countries, with an emphasis on reaching beyond the EU and usual security foresight communities.

Apart from participation in external conferences and workshops, FOCUS organised a couple of dissemination events, including:


- A launch symposium in Brussels;
- A mid-term symposium in Vienna, along with a FOCUS winter school;
- An end-user day in Vienna with a FOCUS on the project's IT aspects; and
- A final symposium in Krems, organised by partner Danube University Krems (DUK).

The development of the turnout for those events shows how FOCUS succeeded to create sustainable end-user interest in its work and results. With the group on “Future SEcurity Research” (FUSER) established in Xing (<http://www.xing.com/net/pri18e2a4x/fuser> ) FOCUS created a platform to keep this community alive.

Outreach beyond the EU were an important objective of FOCUS according to Annex I. Inter-project relations with the U.S. homeland security enterprise established by FOCUS also included dissemination activities on conferences and workshops, in addition to the common foresight work done. Highlights include participation in FEMA conferences and workshops, and in FEMA's Strategic Foresight Initiative (SFI, <http://www.fema.gov/strategic-planning-analysis-spa-division/strategic-foresight-initiative> ) . These activities lead to a transatlantic scenario workshop in Washington, DC that among other things yielded a roadmap track for developing transatlantic research themes in emerging common fields of U.S. Homeland security research and EU security research. These results were included in the FOCUS roadmap proposal for “security research 2035.”

Another example of FOCUS outreach to new and emerging communities beyond those typical of the FP7 Security theme was the project's presentation at the "itsa 2012" in Nuremberg, the leading German IT security fair and congress, attracting more than 5.000 visitors every year. Numerous visitors were informed about FOCUS objectives and results at the booth of FOCUS partner Danube University Krems (DUK),

2 FOCUS special issue of Information & Security – an International Journal

Summarising results from various FOCUS studies, a special issue of "Information & Security" published in February 2013 presents selected results from the FOCUS project. A first group of articles discusses methods and techniques in scenario-based foresight as integrated and applied within FOCUS. A second group of articles presents selected empirical results from FOCUS scenario foresight on threats, risk management needs, and future EU roles as a comprehensive security provider. A third group introduces research planning implications from selected FOCUS security scenarios. A final set addresses the way ahead: how FOCUS methods and results could be useful beyond the immediate mission and scope of the project to guide policy development and industry strategies. The issue is available in full text (<http://procon.bg/volume29> )


3 Use of FOCUS results in other security research projects

Use of FOCUS results in other security research projects in which some FOCUS partners are involved includes, for example, use of FOCUS roadmap tracks as checklists for ethics and societal security aspects in the newly started EU security research project AEROCEPTOR (<http://www.aeroceptor.eu> ) on a remotely piloted aerial system (RPAS) to support police activity. Another example is the utilisation of FOCUS wikis – by FOCUS partners that are universities – in teaching and the use of another roadmap track to upgrade or develop new curricula.

4 Examples of other practical uses of FOCUS results

FOCUS participated in the European Commission's online consultation on security research in Horizon 2020 that was conducted in summer 2012. It submitted its so far reached results in the "Survey on possible research needs in Horizon 2020 'Secure Societies'."

ASFINAG's (AUTOBAHNEN- UND SCHNELLSTRASSEN-FINANZIERUNGS-AKTIENGESELLSCHAFT) internal revision used FOCUS results from the "Big Theme" of "Critical infrastructure and supply chain protection" to prepare for an internal mid-term audit.

Results from FOCUS will be used to formulate inputs into the Ascent Look Out trends (<http://ascentlookout.atos.net/en-us> ) platform from FOCUS partner Atos. Ascent Look Out aims to raise awareness of the emerging trends, business needs, and technologies that will drive innovation, and takes into account socio-cultural, economic and political (SEP) impacts into different business markets and its

trends. Ascent Look Out is updated every year with latest business, technology, and SEP trends. Therefore, thematic results from FOCUS will be used to enrich this tool and provide a more accurate insight in future security trends

5 Matching of main results from FOCUS with conclusions from the European Commission's Security Research Event (SRE) 2013

At the HOMSEC 2013 fair and conference, held in Madrid in March 2013, the European Commission, Directorate General Enterprise and Industry, organised a Security Research Event (SRE2013, <http://sre2013madrid.es> ). Next to discussing industry-related aspects in current and future security research, the event included a panel presentation and discussion about security research in Horizon 2020. FOCUS attended the event in order to gain latest insight about the matching of its results, and the way the presentation of its final results is being prepared, with current perspectives for future security research at European Commission and industry level.

While SRE2013 emphasised the need to familiarise end-users with new and emerging technologies, FOCUS would add that security research should also contribute to educating end-users on the technology-society link, on policy scenarios that the use of technology may have to cope with in the future, as well as on social and cultural contexts of acceptance and use of technology. The FOCUS roadmap proposal can support such an approach by its included curriculum matrix that also comprises an executive education module.

Moreover, from the FOCUS point of view, based on the results of its multiple foresight work, future security research planning should go beyond a mission-centred approach. Future security research should not only help create economic opportunities and positioning the EU on the global market as a provider of security technology. Rather, it should support the EU to make not only enhanced product-related but also enhanced political offerings in a globalised world. Framework programmes are a mechanism, while security should be a reality.

From the industry point of view and related to the European Commission's "Action Plan for an innovative and competitive security industry," the need was pointed out on SRE2013 increase joint-up analyses of security gaps, challenges, and technological requirements, in particular by bringing together industry and end users. This pointed beyond the common FP7 security research approach to bring together research and end-users. It reinforces FOCUS' conclusion that the concept of research to meet pre-defined end-user requirements should be amended in the future and that the path taken in FOCUS can be valuable to follow further. For example, the FOCUS reference scenarios and roadmap include prioritisation of security technology needs as well as of end-user requirements in the world of 2035. In the "end-user memorandum" on the reference scenarios (Deliverable 1.4) – which was written based on online collaboration of representatives from end-user and industry sectors – it was, among other things, concluded that end-user and industry interaction should become more futuristic. That is, it should not only concentrate on what the market has to offer today but also reflect both future policy and future technology changes/innovations for EU security-related activities in 2035, including identification of possible new players.

The need articulated on SRE2013 to for example involve agencies in charge of procurement in security research and demonstrate this research field's uses, with a focus on pre-operational validation, points to a future possible context of use of the FOCUS scenarios and its identified futuristic key technologies. SRE2013's addressing of the relevance of harmonisation of needs and of improved exploitation of public-private partnerships as a tool in the security sector are in line with, and underscore, FOCUS foresight results.

SRE2013 panels moreover focused on creating synergies with defence, following the Lisbon Treaty's abolition of the EU's "three pillar structure" and the creation of the legal base to extend future security research to the "external dimension" of EU security. Addressing new challenges of dual use in this regard, discussion showed another possible additional context of use of FOCUS scenarios: SRE2013 concluded that technology as such cannot be considered civil or military before it is applied to certain needs and/or functions. FOCUS scenarios – in particular from the Big Theme of the "EU as a global actor based on the wider Petersberg tasks " – can provide contexts in which future drawing lines between "dual use" and "military only " – and future security needs and functions that will give technology a civil or military character – can be explored.

6 Socio-economic impact

Indicators for the socio-economic impact assessment of FOCUS are listed in Section 4.3 Tables C to H of this report. Accordingly, the overall employment effect of the project was 25 Full Time Equivalents. 40% of the total project staff were women. A total of 8 persons were hired by beneficiaries specifically for the purpose of the FOCUS project.

7 Wider societal implications

FOCUS overall results reinforce a clear set of criteria for good security research that is conscious of its broader societal impact. For example, security research should include advice to authorities to make appropriate trade-offs between security and other valued societal objectives, while security research projects should make a well defined and tangible contribution to the development of security research as a societally relevant discipline.

Addressing ethical aspects is not only a requirement for good research. It is also of high importance for citizens' perception of the scientific integrity and societal impact of security research. Addressing ethical aspects in security research thus contributes to the social legitimacy of its scientific efforts, as well as society's acceptance and use of its results and products. FOCUS results indicate that there is still a tendency to address ethical aspects via normative means by enacting policies and procedures that reduce the risk of negative ethical and societal impacts.

There is, to begin with, the reluctance of some Member States to connect "Security" with "Inclusive Societies" as an integrated theme of Horizon 2020 research. Instead, the preference has been for

discussion of “Security” as a separate research theme. This may be interpreted as a reluctance to regard security research as a societal enterprise.

On the one hand, a certain amount of security research, however much it is influenced by consultation with concerned parts of civil society, can involve secrecy, or at least restricted information. This is reflected also in some of the security classifications of research deliverables in FP7. Not everything is made public. On the other hand, security research has in the past been under informed by detailed information on societal attitudes to some of the relevant technology, and research on for example the degree and prevalence in different parts of the EU of worry or fear about different kinds of security threat: organised crime in some areas; terrorism in others.

A properly informed and responsive security programme is not necessarily the same as research that is primarily or exclusively social scientific; or that is led by civil society to the exclusion of technology developers and exporters. FOCUS therefore recommends

- Socially informed and socially responsive security research,

where this is different from an entirely new socially formed and social-scientific research science.

Many of the FOCUS reference scenarios, especially the one considering the EU as providing a comprehensive approach to security and security research, raise issues with ethical aspects – from financial and other burden-sharing to tensions between subsidiarity on the one hand and effectiveness and affordability on the other. Since many security research issues are connected with rights regarded as fundamental under the EU constitution but not necessarily with a long history of being respected everywhere, differences in the security and rights traditions of different countries and especially of accession countries compared to more long-standing Member States also need to be addressed in the associated security research.

To be appropriately informed in this regard, security research sometimes requires a special concentration on sections of populations whose attitudes are in transition and to whom historical studies are relevant. This is in line with the FOCUS recommendation that there should be more

- Social sciences and humanities research.

In the reference scenarios in FOCUS concerned with research arising from global climate change, work is envisaged which will emphasise the requirements of disaster prevention, especially from the use of carbon-intensive technologies. This research will certainly raise

- Ethical issues concerning the dependence of prosperity and employment on non-green consumer and other preferences, and what can be done to introduce new green technologies that are socially acceptable. Those technologies include devices to monitor, model, and conserve the environment and natural resources, and to mitigate negative anthropogenic impacts on the environment.

As in other areas of research that connect with the FOCUS reference scenarios, there will be regional

disparities in the adoption of green measures by both business and the public, so that the degree and burdens of adaptation will be greater in some places than others. What permissible measures can be introduced to make the transition to greener behavior both speedy and socially acceptable? How far will this involve economic dislocation? These are questions that indicate some of the ethical dimensions of research on the prevention of a climate-change disaster.

In the case of climate change, security research will have to include recommendations not only of what businesses and governments must do to change, but also how individual behaviour might be encouraged or required to become greener. Metering of energy use is already in force, and this could increase in the era of the “smart home,” especially in urban areas. This might be a socially necessary but perhaps disliked kind of surveillance for the sake of reducing the speed of climate change. Its apparently authoritarian aspects might need to be made the subject of social science research.

Cybersecurity is an important focal point of the reference scenarios, both in connection with critical infrastructures and in general. Since a certain amount of health monitoring in 2035 will be carried out digitally, the security of e-health systems will be important to both governments and populations in the EU. This might be a point of vulnerability to hostile attack or to a sort of blackmail of governments. In such cases, vulnerability is known to be reduced if numbers of networks are multiplied, but this is at the cost of interoperability, which has been a principal focus of FP7 research.

Future security research should thus include a track that focuses on ethical aspects from a more comprehensive point of view, while preserving and enhancing the level of awareness for ethical issues that can arise from security research, and the formal methods to ensure ethical integrity of research.

Furthermore, the FOCUS project yielded self-experience regarding the awareness for effects and wider societal implication of foresight work in security research. It turned out that parts of FOCUS foresight, such as online crowdsourcing of scenario information, exhibited to some extent the character of action research – not only producing knowledge and identifying technological requirements, but changing mindsets and levels of awareness on the side of the experts involved.

However, lessons learned in the project’s foresight exercises include that stakeholders in some cases did not feel that they were in fact users/stakeholders of current or future security research. FOCUS made a contribution to the raising of appropriate awareness.

8 Exploitation of results

9.1 Overview

Exploitation is addressed in Template B2 of the present report. Applying and deploying results, insights, and foresighting scenarios developed in the FOCUS project will be a main goal of exploitation activities by all partners after the project’s lifetime. Integrating the results, especially the foresighting methods will put European consulting agencies and academia at the forefront of the international security communities. Realising this potential is the main goal of the consortium’s exploitation strategy and plan as detailed in

Deliverable 9.7. All exploitation activities are governed by the procedures and Intellectual Property Rights regulations set forth in the FOCUS Consortium Agreement and described in Deliverable 9.3 Chapter 7.

FOCUS project partners, including consultants, editors, and SMEs, are mainly focusing their exploitation activities on improving their expertise, standing, current operation and business position in existing markets and on the creation of and preparation for new challenges, with the intention to secure a strong leadership position in these fields.

FOCUS partners that are universities intend to use FOCUS curriculum-related results to expand or their existing, or launch new, study programmes. Partners expect to raise interest from new sectors of potential students due to their ability to make new course offerings in "new security studies."

FOCUS partners also plan to enter new markets using FOCUS tools, studies, and comprehensive expertise to offer consultancy and services based on foreground generated in the project. This is detailed in Template B2.

It is also expected that FOCUS results can evoke interest on the side of the EU or national agencies to consider them in their planning and implementation activities related to security research in the post-FP7 era. For example, partner DUK expects to be able to conclude long-term consultancy contracts with Austrian federal government bodies. Those FOCUS partners that are also end-users, such as ISDEFE, expect to enhance existing capabilities in technology watch, horizon scanning and foresight, and resulting future opportunities for improving consulting services as well as new opportunities to collaborate in R&D projects.

The following examples illustrate FOCUS exploitation potential and plans per given category:

9.2 General advancement of knowledge

- Publications for expert and citizen education as well as for policy planning: FOCUS team members will work together to identify possible journals/publishers and will collaborate on submission of articles drawn from FOCUS studies/deliverables;
- Practically using FOCUS criteria for good security research and consideration of ethics aspects as summarised in Deliverable 8.4: Providing ethics and social sciences/humanities aspects checklists for other FP7 security research projects, such as AEROCEPTOR.
- Exploiting R&D results academically: scenario questionnaire repository and construction tool as well as wikis on IT-based Knowledge Platform, for use as a knowledge acquisition tool for crowdsourcing of scenario information, online expert collaboration, etc.

9.3 Commercial exploitation of R&D results

- The integration of foresighting methods and tools will provide future opportunities for improving consulting services; enhance existing capabilities in technology watch, horizon scanning and foresight.
- Higher education & professional training, including gaming and exercises.
- Higher education & professional training: Exploitation of all “critical infrastructure and supply chain protection” outcomes of FOCUS project at undergraduate and Executive MBA supply chain courses at HEC University of Lausanne.

9.4 Exploitation of results through EU policies and (social) innovation

- Integrate FOCUS foresighting methodologies and generated foreground into future research proposals and projects: roadmap for scenario-based security research planning; related themes of topics; lists of experts; etc.
- Briefing of policymakers and other stakeholders regarding EU security research planning for Horizon 2020 and beyond – via direct contact with policymaker circles: roadmap for scenario-based security research planning; related themes of topics; lists of experts; etc.
- Public administration: long-term consultancy contracts with Austrian federal government bodies.
- FOCUS methodology, with the two-year practical and academic experience: introducing the foresight methodologies of FOCUS-project to a select groups of experts at the World Customs Organisation (WCO).

List of Websites:

<http://www.focusproject.eu> 

FOCUS Coordinator:

Prof. Dr. Alexander Siedschlag

Sigmund Freud Private University Vienna
CEUSS | Center for European Security Studies
Schnirchgasse 9a
A-1030 Vienna
AUSTRIA

Phone: +43 (0) 1 798 62 90 50

Fax: +43 (0) 1 798 62 90 52

E-mail: siedschlag@european-security.info

Website: <http://www.european-security.info> 

Last update: 1 August 2014

Permalink: <https://cordis.europa.eu/project/id/261633/reporting>

European Union, 2025

