

Syllabus of thematic embedded scenarios

Alternative futures of security research for a comprehensive approach

Deliverable 3.3

Danube University Krems, Austria (DUK)

March 2012

FOCUS is co-funded by the European Commission under the 7th Framework Programme, theme "security", call FP7-SEC-2010-1, work programme topic 6.3-2 "Fore sighting the contribution of security research to meet the future EU roles".



FOCUS (*“Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles”*) aims wide but with concrete policy guidance in mind: namely to define the most plausible threat scenarios that affect the “borderline” between the EU’s external and internal dimensions to security – and to derive guidance for the Union’s future possible security roles and decisions to plan research in support of those roles.

The FOCUS project is co-funded under the Security Research theme of the EU’s 7th EU Framework Programme, for the period of April 2011 to March 2013. FOCUS brings together 13 partners from 8 countries, including universities, industry, think tanks and security information providers. For more information about FOCUS, and to download presentations and multi-lingual project flyers, as well as to access the foresight platform with online questionnaires, please visit the project website at <http://www.focusproject.eu>.

Imprint

Responsible project partner

DUK – Danube University Krems, AT

Contributing partners

CVUT – Czech Technical University, CZ

ISDEFE – ISDEFE, ES

SECEUR – SecEUR – SECURITY EUROPE, BE

U HAIFA – University of Haifa, IL

ATOS – Atos origin SAE, ES

Authors and contact information

Walter Seböck, DUK, walter.seboeck@donau-uni.ac.at

Johannes Göllner, DUK, johannes.goellner@donau-uni.ac.at

Andreas Peer, DUK, andreas.peer@donau-uni.ac.at

Johann Höchtl, DUK, johann.hoechtl@donau-uni.ac.at

Thomas Benesch, DUK, thomas.benesch@donau-uni.ac.at

Dr.Prochazkova.Dana, CVUT, dr.prochazkova.dana@seznam.cz

David Sanchez Garcia, ISDEFE, dsanchez@isdefe.es

Raquel Lozano Bernal, ISDEFE, rlozano@isdefe.es

Rachel Swisa, ISDEFE, rswisa@univ.haifa.ac.il

Brooks Tigner, SecEUR, bt@seceur.info

Ricard Munné Caldés, ATOS, ricard.munne@atosresearch.eu

FOCUS Website

<http://www.focusproject.eu>

Version history

<i>Version</i>	<i>Date</i>	<i>Change/Remark</i>	<i>Responsible (person, beneficiary/function)</i>
0.1	14-03-2012	Initial version	Walter Seböck, DUK Johann Höchtl, DUK
0.2	16-03-2012	Compilation of partner contributions	Walter Seböck, DUK Johann Höchtl, DUK
0.3-0.6	until 29-03-2012	Integration and review	Walter Seböck, DUK Johann Höchtl, DUK
1.0	30-03-2012	Submitted version	Walter Seböck, DUK
7.0	27-04-2012	Revised version for public release	Walter Seböck, DUK Johann Höchtl, DUK

CONTENTS

1	Executive summary	6
2	Concept and objectives	7
3	Selected context scenarios from Deliverable 3.2 (Alternative future models of the comprehensive approach as main reference for exogenous EU roles)	8
3.1	Approach.....	8
3.2	Policy strategies consensus scenario.....	8
3.3	Policy strategies leftovers scenario	9
3.4	Materialism scenario.....	10
4	Future security research thematic tracks	11
4.1	Approach to the identification of thematic tracks	11
4.2	EU cohesion, decision making and governance.....	11
4.3	Willingness to invest in preparedness	11
4.4	Intelligent, knowledge based monitoring of new social media and other open information sources	12
4.5	Integrated situational pictures as facilitation for networked operation and command structures....	13
4.6	Information exchange between civilian and military actors in order to provide common, timely and relevant situational awareness.....	14
4.7	Development of standardised skills and integrated information systems for effective coordination	15
4.8	Training schemes for use of technology, including new social network technologies.....	15
5	Scenarios for alternative futures of security research in support of the comprehensive approach	17
5.1	Approach.....	17
5.2	Scenarios for Security research 2035 in support of the EU as a comprehensive security provider	18
5.2.1	<i>Generalised security research system</i>	18
5.2.2	<i>Nationalisation of security research</i>	18
5.2.3	<i>Research system for European critical infrastructure protection (EUCIP)</i>	18
5.2.4	<i>Security incident management research</i>	19
5.2.5	<i>Security economics research system</i>	19
5.2.6	<i>Public health research system</i>	19
5.3	Scenario space	20
6	Transversal aspects	21
6.1	Approach.....	21
6.2	Future fields of action and needed expertise.....	21
6.2.1	<i>EU cohesion, decision making and governance</i>	21
6.2.2	<i>Regional/International/global distribution of wealth</i>	21
6.2.3	<i>Dependency on technology with a focus on information and communication technology</i>	21
6.2.4	<i>Methodologies to integrate data from various sources and the human factor</i>	22
6.2.5	<i>Intelligent, knowledge based focusing and filtering functions for new social media and other open information source monitoring</i>	22

6.2.6	Training schemes for technology use including new social network technologies.....	24
6.3	Overcoming present and future weaknesses in comprehensive crisis management	24
6.4	List of experts	26
7	Summary of scenario space description (Common Analytical Framework Matrix)	31

ANNEX

Descriptions of the cells in the Matrix in Table 1	44
--	----

FIGURES AND TABLES

<i>Figure 1:</i> Scenario level addressed in this deliverable.....	7
<i>Figure 2:</i> Scenario space for alternative futures of security research in support of an “EU comprehensive approach 2035”	20
<i>Table 1:</i> Matrix for qualitative description of combination of thematic tracks (as drivers) and context scenarios from Deliverable 3.2	17

1 EXECUTIVE SUMMARY

This deliverable presents scenarios about alternative futures of security research to support a comprehensive approach of the “EU 2035” as a civil security provider. Three scenarios from Deliverable 3.2 (Alternative futures of the comprehensive approach as an organizing context for future EU roles) were selected as context scenarios for the present work, based on weighing along two dimensions: (a) nation/member state vs. EU-level/international approach to civil security and security research; (b) position of the scenario on the continuum of internal/external security. The three selected context scenarios were lined up with identified drivers in a matrix procedure. A matrix for structured description of thematic tracks and scenarios is presented, and extensive qualitative descriptions are provided in the annex.

The scenarios for security research 2035 in support of the EU as a comprehensive security provider were defined based on seminar work of the Winter School, where also the core descriptions for the scenarios were developed. In addition, transversal aspects that relate to future fields of actions and needed expertise were identified in most of the scenarios of “EU security research 2035,” including identification of tools and systems for comprehensive crisis management. Future tracks for security research in the specific context of the comprehensive approach in particular relate to EU cohesion, decision making and governance; investment in preparedness; knowledge-based monitoring of new social media and other open information sources; integrated situational pictures as facilitation for networked operation and command structures; information exchange; standardised skills and integrated information systems for effective coordination; training schemes for use of technology, including new social network technologies.

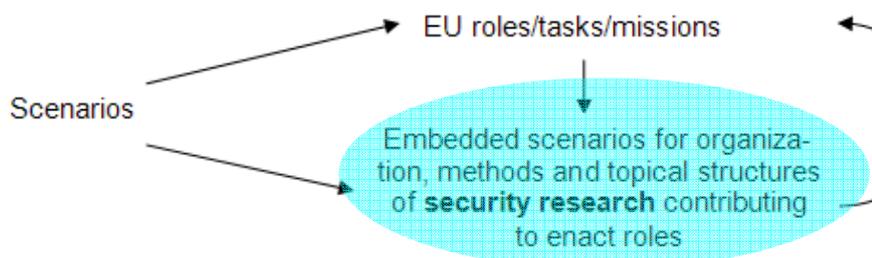
2 CONCEPT AND OBJECTIVES

This deliverable presents scenarios about alternative futures of security research to support a *comprehensive approach* of the “EU 2035” as a civil security provider. In addition, a matrix for structured qualitative description of thematic tracks as drivers and scenarios is presented, and extensive qualitative descriptions are provided in the annex.

The scenarios for security research in the 2035 time frame are developed within the context of three scenarios selected from [Deliverable 3.2](#) (Alternative futures of the *comprehensive approach* as an organizing context for future EU roles), based on weighing along two dimensions: (a) nation/member state vs. EU-level/international approach to civil security and security research; (b) position of the scenario on the continuum of internal/external security.

Figure 1 illustrates the scenario level address in this deliverable:

Figure 1: Scenario level addressed in this deliverable.



The three selected context scenarios are lined up with identified drivers in a matrix procedure, based on interviews with internal as well as external experts. Interim results were discussed on the FOCUS project’s Winter School ([Deliverable 9.4](#)). The scenarios for security research 2035 in support of the EU as a comprehensive security provider were defined based on seminar work on the Winter School, where also the core descriptions for the scenarios were developed.

The deliverable also identifies a list of cross-cutting, or “transversal” aspects that generally all of the developed six scenarios for “security research 2035” have in common. Those transversal aspects relate to future fields of action and needed expertise in most of the six future scenarios for “security research 2035”, including identification of tools and systems for comprehensive crisis management to overcome present and anticipated future weaknesses. Based on these results, a list of experts is provided whose qualification and experience may be useful to address anticipated thematic gaps and challenges for “security research 2035”.

3 SELECTED CONTEXT SCENARIOS FROM DELIVERABLE 3.2 (ALTERNATIVE FUTURE MODELS OF THE COMPREHENSIVE APPROACH AS MAIN REFERENCE FOR EXOGENOUS EU ROLES)

3.1 APPROACH

[Deliverable 3.2 \(Report on alternative future models of comprehensiveness\)](#) developed scenarios from FOCUS foresight processes that included conceptual analysis and scholarly work as well as empirical work. Empirical work was based on quantitative conceptual analysis, expert questionnaires, and guided interviews. The level of analysis addressed were context scenarios (future concepts of the *comprehensive approach* as main reference for exogenous EU roles).

From the scenarios presented in Deliverable 3.2, the following three were selected, based on results of internal project workshops and in accordance with their relevance to tangible future security research themes in the 2035 time frame of the project. Scenario selection also followed the principle of integration of expert and policy scenarios. The following scenarios and the analyses that yielded them are described in [Deliverable 3.2 \(Report on alternative future models of comprehensiveness\)](#).

3.2 POLICY STRATEGIES CONSENSUS SCENARIO

This scenario rests on the assumption that politically planned/desired futures of comprehensiveness are going to materialise as foreseen in relevant strategic documents. In this scenario it is essential to define, which measures must be taken within the EU in order to find solutions on the basis of participation and ownership as well as common shared values.

The *comprehensive approach* is widely understood as a method for coordination of crisis response between autonomous actors. It is intervention-based and top-down: The EU 2035 brings solutions to problems, without much emphasis on participation, ownership or the “whole of community” principle. The *comprehensive approach* involves no common sources, but rests on clear rules for division of labour between all actors involved and sometimes includes international combination of capabilities and pooling. Actions that are taken are soundly based on integrated risk assessment and coordinated decision making, including more decision-making power for EU institutions and bodies, who can occasionally override Member States’ opposing national interests.

Based on extended experience with occasional use of military within the Union (such as securing VIP and big sports events), the EU 2035 has developed a common doctrine for the use of military assets under EU mandate in preventive and other operations on Member State territory. It also focuses on a hazard-driven policy and capability process, based on integrated assessment and decision-making, which has transcended the security-safety divide and broadened EU and Member States security strategies to encompass both.

Main question for future security research in the context of this scenario

- “What measures must be taken to ensure that individual states cannot override common rules for hazard-driven policy?”

3.3 POLICY STRATEGIES LEFTOVERS SCENARIO

This scenario encompasses the assumption that initiatives will emerge to complement unaffected aspects of the future EU security role and is essential for a true *comprehensive approach* of the EU as a security provider.

The *comprehensive approach 2035* has been considerably developed further and expanded, in terms of concepts, policies, and methods. For 2035 policies are being drafted to overcome one-sided views and structural pitfalls of the approaches of the 2010s. Strategic threats by the EU are not regarded as self-evident, and the definition of EU security and threats is seen related to groups of experts, communities of practice, and collective social processes that construct and assign specific meanings to threats. This is one of the reasons why broad, inclusive foresight involving various stakeholders from within and outside the EU as well as more “technological” comprehensive risk assessment are applied in the EU security strategy processes. In this context, the distinction of (information) technology, for example, as primarily civilian or military in character and use, has become almost completely blurred, with research and development as well as procurement not being planned, undertaken or assessed along the civil-military line.

The EU 2035 and its Member States place much emphasis on the building of resilience and ownership at the citizen level, as well as in the EU’s neighbouring countries and the broader international environment. This is reflected in a system that the EU has established and that joins up significant number of partners in operations, including international and regional organisations, nations, and NGOs. Also, the EU 2035 firms up its decision making by a common operational picture process that has been established on the EU level, based on firm agreements about information sharing, and fully considers the internal-external threat/security continuum. In its action, effects-based approaches, international joining of forces and improvement of general political and societal acceptance at home and abroad are important to the EU and its decision makers.

At the same time, in its exogenous roles to counter threats before they reach the Union and its citizens, the EU acknowledges that there is no one-size-fits-all approach – especially with regard to civil-military interaction as a core part of the *comprehensive approach* that varies in intensity and quality, and ranges from cooperation to coordination to coexistence. The EU 2035 also acknowledges that cooperation is not always possible or wanted by all Member States, EU bodies or international organisations, and that divergent perspectives, missions and goals as well as cultural, social, and political differences make cooperation between military and some civil organisations very difficult to achieve in EU external actions, encompassing security missions, diplomacy or disaster response actions.

Core of the concept of comprehensive security

- Forward-looking (as opposed to problem-solving); mainly refers to integrated assessment (common operational picture along the internal-external threat/security continuum; use of foresight).

Main question for future security research in the context of this scenario

- What measures must be taken to review and integrate interdisciplinary expertise in European security policy?

3.4 MATERIALISM SCENARIO

This scenario foresees a common pragmatic practice of comprehensive security along the security-safety continuum. This pragmatic practice is largely determined by temporarily prevalent concepts for civil-military interaction. In this scenario, it is essential to define a possible way of close cooperation and harmonisation among the EU Member States to achieve better results concerning strategy and operations in the area of security.

The EU has slid into the common pragmatic practice of comprehensive security that covers the whole security-safety continuum, yet, - without much of a strategic background - let alone a vision. This pragmatic practice is largely determined by temporarily prevalent concepts for civil-military coordination (political-strategic and operational level), and available/usable capabilities/instruments in other sectors, including political, diplomatic, economic, intelligence, judicial, and non-governmental areas. The role of the EU is that of a generator, mobiliser, collector, or provider of partnership and cooperation in order to reach a comprehensive response to the security case in question. There are some indications that for the effective use of all of these instruments, a higher functionality, harmonisation and possible integration could be accomplished within the EU, but this is not very clear yet.

Nevertheless, the full implementation of the solidarity clause provides a good basis, in particular as related to prevention of terrorist threats in Member States' territory and the protection of democratic institutions from terrorist attack. An important factor in this process is the closing of gaps in ICT-related interoperability and coordination, not only within but between international organisations.

Cyber threats have proliferated and opponents have acquired capabilities to organise high-consequence attacks against European critical infrastructures. Related to common assessments of cyber threats in particular, "mixed" civil-military capabilities have been developed and pooled on the EU level in the form of partnership between EU bodies and private actors, which is based on early-stage definition of requirements. For example, several Member States have merged their computer emergency response teams (CERTs) into a supranational EU team. However, increasingly scarce resources could limit national divergences and increase support for powerful coordination and pooling of resources on the EU level. EU bodies already have stringent policies to support and enhance cross-national initiatives and practices, in order to increase the effects of existing potentials and instruments without expending more money or effort to increase their impact. Appropriate internal EU structures are in place, allowing the Union to perform complex civil-military tasks in crisis management.

Main questions for future security research in the context of this scenario

- Do you believe that an enhanced cooperation and harmonisation could reduce or optimise resources in partner countries?
- What kind of harmonisation and cooperation is preferred or defined as useful?

4 FUTURE SECURITY RESEARCH THEMATIC TRACKS

4.1 APPROACH TO THE IDENTIFICATION OF THEMATIC TRACKS

Thematic tracks are based on results from [Deliverable 3.2](#). They were adapted according to expert assessments from FOCUS partners as well as seminar discussions during FOCUS Winter School and also conceptually used as drivers for developing the scenarios on alternative futures of security research.

The thematic tracks were also used in the matrix for qualitative description of combination of thematic tracks as drivers and context scenarios.... ([Approach](#)).

4.2 EU COHESION, DECISION MAKING AND GOVERNANCE

It is critical to generate standardised procedures and instructions for actions in line with the concepts of simplification and rapid availability of forces. In addition, a corresponding standardised integrated concept of interventions/missions has to be generated for the decision making process. This has to be defined, tested and implemented on a political, managerial and technical level. Furthermore, standardised operational procedures (SOPs) and rules of engagement (RoE) have to be defined.

These SOPs and RoE have to be examined, adapted and taken into account for compliance with legal stipulations of different Member States. Therefore, possible European missions are easier and more reliably guaranteed in terms of a *comprehensive approach*. Harmonisation of legal frameworks and technical standards are essential for planning, implementation and evaluation.

Currently RoE and SOPs are defined and determined according to the intervention and its participating countries. Therefore specific SOPs/RoE apply to each intervention. Standards based on a portfolio of scenarios and instructions for action have to be prepared for effective and efficient intervention (mission) planning, implementation and evaluation. The EU's approach to this is: (a) define a catalogue of requirements; (b) define a catalogue of force; and (c) derive a final catalogue of capabilities. Future research could develop strategic scenarios with foreseen postures to help move the process of capability generation beyond a case-to-case level.

4.3 WILLINGNESS TO INVEST IN PREPAREDNESS

Security is perceived as an essential characteristic of advanced, developed and democratic countries. The will to invest in preparedness is high. Each EU member state has the obligation to protect its citizens. As such, willingness is not a factor that goes into preparedness on national security issues – it is a legal obligation. The extent to which it is elaborated is determined by the national resources available (expertise, manpower and funding) and the EU has little say over that, except to urge the Member States to follow its recommendations and to provide certain levels of funding to help them do that. Moreover, “national security” also covers military affairs, where the EU has absolutely no say or control over national decisions.

To illustrate this, the Spanish Security Strategy¹ for example states: “Ensuring the security of Spain, its inhabitants and its citizens is an essential responsibility of the Government and the Public Administrations, but also of society as a whole. Security today is everyone’s responsibility.” The strategy mentions some strategic lines of action for each of the areas, (armed conflicts, terrorism, organised crime, financial and economic insecurity, energy vulnerability, proliferation of weapons of mass destruction, cyber-threats, uncontrolled migratory flows, emergencies and disasters, critical infrastructures, supplies and services) but with no concrete commitment of investment to any of them.

Preserving security requires international and national coordination as well as the involvement of society as a whole. Member States are aware they can be more influential in the world if they negotiate their interests at the level of the European Union instead of as a single country, so in the future the Union will have a role in finding common interests and investing smartly, but in the case there is not a common interest multilateral agreements will be elaborated.

At the same time some trends reduce the potential effectiveness at both national and European levels. The most important current trend is the economic crisis which is reducing security investments of the EU Member States and consequently weakening the prospects for a European *comprehensive approach* based on Member States resources. “Smart civil security” initiatives will therefore be of interest to most countries and pose a new topic for research.

4.4 INTELLIGENT, KNOWLEDGE BASED MONITORING OF NEW SOCIAL MEDIA AND OTHER OPEN INFORMATION SOURCES

At the Techonomy Conference 2010, Eric Schmidt, CEO of Google said that every two days now we create as much information as we did from the dawn of civilization up until 2003 [...] That’s something like five exabytes of data. This statement underlines what can be perceived from any connected individual: information society is struggling to separate noise from relevant information. This imposes an enormous challenge for policy makers. On the one hand, the sheer amount of data and information should theoretically allow for more informed and better decisions, yet it has become increasingly difficult to identify what is important and what is not.

The information revolution resulted in new flows of data, information, and knowledge. Social networks have grown stronger as forms of organisation of human activity. Social networks are nodes of individuals, groups, organisations, and related systems that tie in one or more types of interdependencies. Social networks mainly carry two forms of information: structural information, who is connected with whom, and information payload regarding the actual information exchange between groups and individuals.

European political leaders and decision-makers, both at national and EU level, are acutely aware and concerned about the impact of social media and other open-source information channels on security-related events (social unrest, disasters, terrorist acts, demonstrations, etc.) – and how the use of these media (whether by members of the public or the authorities themselves) could mitigate or shape perceptions and reactions to a given event.

At European level the EUROSINT Forum (<http://www.eurosint.eu>) is dedicated to European cooperation and use of open source intelligence (“OSINT”) that prevents risks and threats to

1 Spanish Government: *Spanish Security Strategy* (2011). Retrieved from: <http://www.lamoncloa.gob.es/NR/rdonlyres/EF784340-AB29-4DFC-8A4B-206339A29BED/0/SpanishSecurityStrategy.pdf>.

preserve peace and security. In the future, standardisation of architectures and components for open source intelligence applications will be required to enable interoperability. At the same time, respect for privacy and fundamental rights has to be present to determine the requirements imposed by legislation and design constraints that assure compliance and citizens' acceptance.

In Spain, for example, a national initiative called IBEROSINT, with the support of Spanish Ministry of Interior, is active in gathering security users with interest in open source intelligence for security, in order to define common requirements, needs, cooperation and to be aware of the current products and developments, some of them are in R&D phases such as the FP7-SEC-2008 project VIRTUOSO (<http://www.virtuoso.eu>). The Spanish Security Strategy suggests developing an economic intelligence system for collecting and analyzing financial, entrepreneurial and economic information relevant for the security sector, allowing the detection and prevention of actions against Spanish interests and supporting the action of the State and a better decision making in this ambit.

Modern information and communication technologies enable direct involvement. Virtual social networks such as Facebook, Twitter and Google+ easily support connections to thousands of people, across social levels and age groups. The relative ease of using such platforms has resulted in a proliferation of information, which requires substantial infrastructural investments from the platform providers. The more relevant information at hand, the better decisions can be made. Better in this respect means to make more effective decisions by using a minimum of required resources efficiently. Brute force methodologies to extract security-relevant information will fail by the linear runtime behaviour of such approaches. Two main topics for research arise:

- Relevance: How to identify relevant information from noise?
- Completeness: How to reach a level of certainty that all relevant information got extracted?

Multinational enterprises, largely beyond the EU's jurisdiction, provide platforms where millions of people all over the world gather and exchange information (Facebook: 820 million registered users 2012, <http://www.checkfacebook.com>), almost without any regulation. It has been acknowledged by government entities that both structural information ("who is connected with whom") and information payload are valuable resources for risk prevention and trend analysis in order to make more forward-looking decisions. In Australia, for example, Twitter is already actively monitored by first responder organisations to spot those points where people are actually at risk of fire or flooding.

Thus an addition prior security research topic emerges: Policies are required at the highest possible level to take use of information in social networks, to improve external communications and outreach, to raise situational awareness and for practical operational use.

4.5 INTEGRATED SITUATIONAL PICTURES AS FACILITATION FOR NETWORKED OPERATION AND COMMAND STRUCTURES

Hard and actual concrete binding linkages between EU member state communication and command structures do not exist. What does exist are: nascent (newly-created) common operational pictures between certain groupings of national militaries – but on a voluntary basis. For example, 15 Member States navies are building a common operational picture for maritime surveillance – a capability that will eventually be shared with all EU Member States. National air forces are able to do this already, but only via the networks of NATO.

Elsewhere, EU research and technology initiatives such as Galileo, GMES and other projects aim to establish common pictures across land, shore, ship and satellite-based platforms to create situational awareness along all the EU's external borders. This information will feed into national and EU decision-making to help shaping security policy decision-making, though nothing has been formally agreed on yet.

All the above are ripe topics for future research into the impact of these technological advances on the EU's future policies and their implications for security.

Currently the FP7-SEC-2009 demonstration project PERSEUS (<http://www.perseus-fp7.eu>) aims to build and demonstrate an EU maritime surveillance systems integrating existing national and communitarian installations and enhancing them with innovative technologies. PERSEUS is therefore a key project for delivering comprehensive maritime surveillance from coastal regions to high seas through Member State collaboration.

Integrated situational pictures, networked operation command structures, and other related terminology are derived from the military domain and result from legal framework agreement between Member States. As conflicts in security domain are required to involve both military and civilian resources, military terminology and concepts are shifting to the civil domain, but there are some gaps to fill in the civil organisms to equip them with these tools. Moreover, the sharing of information between the EU's Situation Centre (SITCEN) and civilian players (especially NGOs) is legally not possible. Its favourable evolution is unlikely for matters related to security of information and national security.²

A huge effort has to be done to provide all the relevant organisations with efficient means to interoperate, in order to have a comprehensive situational picture at the highest level in the EU. Specific Situational Pictures and Networked Operation Tools for the civil sector will be required for each relevant organisation, posing real challenges for future security research.

4.6 INFORMATION EXCHANGE BETWEEN CIVILIAN AND MILITARY ACTORS IN ORDER TO PROVIDE COMMON, TIMELY AND RELEVANT SITUATIONAL AWARENESS

At the EU level, even if civil-military information exchanges are widely considered necessary for a "comprehensive" operational picture in theatre, the concept is perceived as controversial among civilian stakeholders (NGOs, international aid organisations, government development agencies, etc.). Historically, exchanges of information between civil-military actors in theatre have been – and probably will continue to be – unofficial, ad hoc and tailored to the situation at hand. EU crisis management, military and humanitarian officials interact within the European External Action Service (EEAS), which aims to tighten information exchanges across these diverse stakeholders. However, the problem is to get information from non-EU actors – i.e. international organisations and NGOs – during a given operation. They are very wary about doing this with any military entities. Future scenarios for research in this area probably should focus on two things:

- How might *limited (or masked)* exchanges of information take place between civil and military entities to provide each with at least a minimal functioning common operational picture?

2 See the EEAS Crisis management platform in <http://www.consilium.europa.eu/eeas/security-defence/capabilities/crisis-response/eeas-crisis-platform> or the EU Situation Room in <http://www.consilium.europa.eu/eeas/security-defence/capabilities/crisis-response/eu-situation-room>.

- What are the security impacts/consequences for an EU mission – and/or EU security policy in general –if this was achieved?

4.7 DEVELOPMENT OF STANDARDISED SKILLS AND INTEGRATED INFORMATION SYSTEMS FOR EFFECTIVE COORDINATION

The Spanish Security Strategy is a good example for the definition of practically relevant domains, including research tracks for integrated information and cooperation between EU Member States. It identifies the following thematic areas:

Terrorism: Anticipating the development of terrorist actions. This requires to increase the coordination of the services that integrate our intelligence community and cooperation with the European Union, its Member States and other allies.

Organised crime: Improving information and intelligence systems against organised crime in its different forms. The Intelligence Centre against Organised Crime (CICO) has been created with criminal intelligence and operational coordination functions. It integrates the National Police Force and the Civil Guard, with the participation of Regional Police, the Customs Surveillance Service and the Armed Forces as needed. It also aims to improving the coordination between national and international organisations, through communication with the police and intelligence services from other countries, and by reinforcing inter-institutional cooperation. Joint operations with the EU will allow access to data and information and will facilitate exchange with other specialised services.

Financial and economic insecurity: Within the domestic sphere, and in line with what has been done in other countries, a Financial Intelligence System will be established to analyse and provide relevant, timely and useful economic, financial and business information to support the actions of the state and enable better decision-making. This System will make knowledge sharing easier, create synergies, avoid redundancies and facilitate the adoption of common positions within public administration. In close cooperation with different economic actors, it will contribute to state security tasks by helping to identify and prevent actions that are contrary to Spain's economic, financial, technological and commercial interests in strategic sectors.

Cyber threats: Combat cyber threats at a European level by expanding and consolidating existing means. In 2004, the European Network and Information Security Agency (ENISA) was established for the double purpose of achieving greater security in EU networks and information, and facilitating the development of a network and information security culture for the benefit of society as a whole.

Uncontrolled migratory flows: Effective control and surveillance of access to the EU's external borders, within the framework of the EU Integrated Management System for External Borders.

4.8 TRAINING SCHEMES FOR USE OF TECHNOLOGY, INCLUDING NEW SOCIAL NETWORK TECHNOLOGIES

Technology has become the backbone of communication. More and more communication systems are using the IP stack as the data link layer, bridging heterogeneous communication systems and integrating dislocated organisations into virtual entities. Profound knowledge of the technological principles and the resulting social interaction patterns are necessary to fully utilise communication systems at the highest possible level.

Social networks play an 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 and officials, incompatible with the traditional training material to account for the networked and interconnected nature of social networks.

The strength of modern communication systems is their relative independence of homogenised appliances. Most systems rely on well-defined standards like the TCP/IP stack or the GSM/G3/G4 mobile radio stack. Vendors use these protocols as a basis for enhanced services. Highly sophisticated sites like Facebook or gadgets like smart phones still use a technology stack that is more than 15 years old. The federated nature of Europe's administration therefore results in compatible, yet different communication technology infrastructure and end user applications. Therefore training schemes for technology use, including new social network technologies, have to be established on a localised basis. Local authorities require tailored training materials for their officials to fully exploit the capabilities of the technology infrastructure.

Future security research should contribute to developing and implementing training schemes in particular in the following two areas:

- Social media usage: Training material concerning social media usage has to deal with the peculiarities of social networks compared to other media, either electronic or traditional ones. What networks do exist, what is their respective netiquette, what are dos and don'ts? Where to draw the line between official appearance and private position? How to counter public offence by best exploiting the tools capabilities?
- Social media analysis: Social networks are tools to easily disperse and receive information and to manage contacts. However, listening to the crowd is an effective mean to proactively react to threats. Several case studies highlight the precarious aspects to social media, and concerns around monitoring and control by authorities especially during political crises.

5 SCENARIOS FOR ALTERNATIVE FUTURES OF SECURITY RESEARCH IN SUPPORT OF THE COMPREHENSIVE APPROACH

5.1 APPROACH

The scenarios for alternative futures of security research in support of the “*comprehensive approach 2035*” were developed with the use of the matrix shown in *Table 1*. This matrix provides a structure for the qualitative description of combinations of thematic tracks as drivers and context scenarios from [Deliverable 3.2](#). The extensive qualitative description is contained in the *Annex*.

During two internal team workshops of the FOCUS consortium, the context scenarios from *Deliverable 3.2* were analysed and critically assessed and weighed by FOCUS subject matter experts. The weighing was done according to relevance from a dual perspective: (a) nation/member state vs. EU-level/international approach to civil security and security research; (b) position of the scenario on the continuum of internal/external security.

As a result, the three scenarios from *Deliverable 3.2* (Alternative future models of the comprehensive approach as main reference for exogenous EU roles) were selected as context scenarios for alternative futures of security research.

These three selected context scenarios were lined up with drivers identified in *Deliverable 3.2* in a matrix procedure. This was done based on interviews with internal as well as external experts.

The resulting matrix was then compiled via question and feedback loops within the FOCUS consortium. Interim results were discussed during the FOCUS project’s Winter School (see [Deliverable 9.4](#)). The Winter School offered an excellent opportunity for this work in its thematic parallel sessions.

The scenarios for security research 2035 in support of the EU as a comprehensive security provider, as described in the following sub-chapter, were defined based on seminar work during the Winter School, where also the core descriptions for the scenarios were developed.

Table 1: Matrix for qualitative description of combination of thematic tracks (as drivers) and context scenarios from Deliverable 3.2.

Drivers identified in Deliverable 3.2		Cell numbers (qualitative results described in the Annex with reference to those cell numbers)														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Context scenarios	Policy strategies consensus scenario															
	Policy strategies leftovers scenario	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	Materialism scenario	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45

5.2 SCENARIOS FOR SECURITY RESEARCH 2035 IN SUPPORT OF THE EU AS A COMPREHENSIVE SECURITY PROVIDER

5.2.1 *Generalised security research system*

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

5.2.2 *Nationalisation of security research*

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

5.2.3 *Research system for European critical infrastructure protection (EUCIP)*

Security research 2035 is a system on the EU level that focuses on supporting European critical infrastructure protection by technological innovation in order to guarantee interoperability between systems and data, including non-technological strategies to develop effective coordination of security related national bodies at the European level for managing and coordinating effective information exchange for issues like terrorism, financial and economic insecurity, cyber threats, uncontrolled migrations, emergency and civil protection, organised crime, health (early detection of epidemics), intelligence, etc. A main security research issue 2035 is data integration: the extent to which standardisation is used across multiple organisations or sub-units of the same organisation. Data integration provides the benefits of improved managerial information for communication,

improved operational coordination across sub-units or divisions, and improved strategic planning and decision making. However, data integration can also increase costs by increasing the size and complexity of the design problem or increasing the difficulty in getting an agreement. Therefore, choosing the appropriate level of data integration may require trading off coordination against decreased local flexibility and local effectiveness. Orthogonal disciplines, combining time series analyses, visualisation methodologies, and combined network and sensitivity analysis are required to prepare highly heterogeneous data sets for further use as integrated analysis. This task requires a combined bottom-up approach, connecting academic disciplines for broad inclusive foresight involving various stakeholders from within and outside the EU.

5.2.4 Security incident management research

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

5.2.5 Security economics research system

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

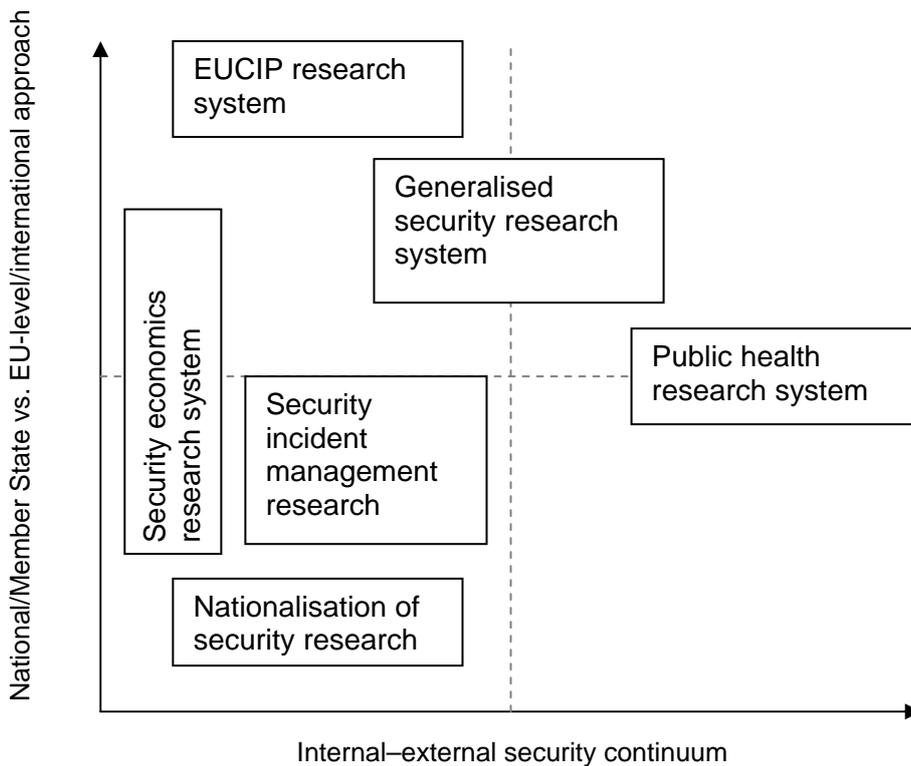
5.2.6 Public health research system

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

5.3 SCENARIO SPACE

Based on the two dimensions that were also used for the analysis of *Deliverable 3.2* results and their uptake in this deliverable, the six alternative futures for security research in support of an “EU comprehensive approach 2035” can be located in the scenario space shown in *Figure 2*.

Figure 2: Scenario space for alternative futures of security research in support of an “EU comprehensive approach 2035”.



6 TRANSVERSAL ASPECTS

6.1 APPROACH

The FOCUS project team identified a list of cross-cutting, or “transversal” aspects that generally all of the six scenarios for “security research 2035” described above have in common. This list is based on work with results that were handed over from [Deliverable 3.2](#).

Those transversal aspects relate to future fields of action and needed expertise in most of the six future scenarios. They are described in *Chapter 6.2*.

In addition, foresight work from FOCUS partner Czech University in Praha (CVUT) on tool and systems for comprehensive crisis management to overcome present and anticipated future weaknesses is introduced.

Based on these results, a list of experts filtered from the project’s various experts-lists is provided.

6.2 FUTURE FIELDS OF ACTION AND NEEDED EXPERTISE

6.2.1 *EU cohesion, decision making and governance*

In the future, it will be difficult to realise simultaneously the objectives of the EU as whole and Member States’ interests. It can also be expected that the EU as well as some national agencies will develop and follow their own interests. This will challenge rapid collective EU action. The following two research lines appear of particular future interest:

- Tools for policies and national views integration,
- Standards for national organisation for a *comprehensive approach* to security.

6.2.2 *Regional/International/global distribution of wealth*

Socio-demographic developments across the European Union have an impact on its overall development, as well as on its capacity to act and on the effectiveness of its instruments. The development and adaptation of relevant legal compliance framework should be based, among other things, on socio-demographic scenario planning. This planning should be comprehensive in that it overarches Member States’ and EU levels, focusing on coordinated goal-oriented action.

6.2.3 *Dependency on technology with a focus on information and communication technology*

A minimum standard for information and communication technology networks and supply chains should be stipulated to ensure that appropriate actions can be taken efficiently and effectively, as well as applied permanently. This minimum standard would define relevant and significant planning scenarios for a *comprehensive approach*, taking into account cascades of risks and impacts. This would also lead to specific requirement profiles, including resources, for EU security roles.

6.2.4 Methodologies to integrate data from various sources and the human factor

Semantic data integration is a technically intense, combined approach, including text frequency analysis, relatedness of concepts, statistic methods and rule based approaches. This complexity and the fact that results will be fuzzy by nature raise concerns about the applicability of semantic methodologies for data integration. While theoretically usable for very heterogeneous data sets, computational complexity makes the application of these methodologies unfeasible. “Big data” has become the buzzword for methodologies to reduce complexity by mapping a data integration problem onto different problem solvers (map-step) and integrating those reduced results back into the actual problem to solve (reduce-step). Companies like Google, Facebook and Twitter apply those technologies at the cost of marginally inaccurate results. Those systems are eventually consistent, but no formal guarantee can be given.

Data integration in the future seems like a problem still best solved by humans. Government bodies hold an enormous amount of data which carries the potential to raise security, welfare, trust and create new economic opportunities. Open data released by government bodies gets inspected, analysed and interpreted by interested volunteers, who in turn create new information. This highly heterogeneous data is best analysed by voluntary stakeholders, like citizens, making available their domain knowledge. Security research might profit from such an approach by dividing analysis and research problems into well-defined portions which get released to the public, accompanied by incentive measures to assure uptake.

All relevant parameters and variables have to be defined and described within European wide information and knowledge management. This is the basis for the concept, modelling and development of a pan-European security information architecture. With this system, all aspects of a *comprehensive approach* could be covered and integrative planning of security interventions, their implementation and evaluation supported. This information architecture could form a basis for a command and control system and enable simulation of multifaceted scenarios.

6.2.5 Intelligent, knowledge based focusing and filtering functions for new social media and other open information source monitoring

Typically, social network analysis relies on questionnaires and interviews to gather information about relationships within a defined group. However, with digital social networks inviting everyone to participate, a redefinition of the term “friendship” or no privacy at all (Twitter, with the exception of private messages), social network analysis can be completely detached from the individuals to be analysed. Key stages of the basic process typically involve the following:

- Define the objective of the analysis;
- Formulate hypotheses and questions;
- Follow/monitor relevant terms or individuals. This step may be supported by a social network monitoring tool;
- Export and convert the data from the monitoring tool;
- Use a social network analysis tool to visually map out the network.

Linkage and flow of information is of particular interest for social network analysis. The analysis gives indicative results of power and influence that individuals have within a certain network. Those results may be used to monitor for example terrorist, first responder and victim activities by location, terrorist group, and to identify trends.

Information payload on the other hand is required to analyse trends, anticipate events or quickly respond to incidents. In this respect the Twitter social network is especially interesting as it is a very informal network, encouraging people to post short messages. A normal tweet is about the size of an SMS that is why information gets frequently abbreviated or shortened by acronyms. Twitter has the notion of “followers”, yet the more powerful feature is to establish ad-hoc relationships by using hash tags (#), responding to a tweet by using the acronym “RT: user <text>” or simply by reposting a message by a user, implicitly raising awareness on the re-tweeted topic.

Another important aspect is the use of URLs within Twitter. The restriction of Twitter messages to 140 characters requires users to shorten links to interesting sites or hotspots using URL shortening services like bit.ly, or goo.gl. As Twitter has almost no notion of privacy (tweets are either directed to the public or to dedicated person, while the later feature is seldom used), questions of data protection can be more easily handled as would be the case with Facebook or Google+. Thus content analysis of Twitter involves the following steps:

- Establish search terms or people to monitor;
- Collect the data using a monitoring tool in an external system: as Tweets are ephemeral and tend to vanish after seven to 14 days, these have to be collected using a predefined external data store. As information in Twitter is not merely expressed by the written word but also through #hash tags, the monitoring system has to dynamically adapt the search criteria and constantly follow users who created new hash tags;
- Data analysis. This step involves traditional text corpora analysis like stop word elimination, text frequency analysis, thesaurus, and semantic methodologies may be used to cluster relevant terms.

The unstructured nature of tweets imposes significant challenges to data analysts. Mobile devices with Twitter clients do have the capability to automatically add location based information (latitude and longitude). This service does not work reliably as some time is required to establish a GPS satellite connection, time which is seldom available during an emergency case where people hastily tweet their despair because of flooding or fire. Thus street and town names have to be extracted from the tweets and mapped by services like geonames.org.

Social media, including Facebook and Twitter, play an increasingly important role in crisis communication, also in natural disasters. This has implications for the practical work of emergency services and media organisations, as well as for further scholarly research. Social media can play an important role in crisis communication and emergency management, and the wider user community is generally willing to support and assist the work of emergency services if that work is undertaken in a way that is compatible with the established community conventions of the social media platform itself. The use of social media for crisis communication is still emerging, and remains largely ad hoc. Emergency services should review their current social media presences, and develop more comprehensive, flexible strategies for using social media in times of crisis. Crucially, this also involves further staff training in using social media effectively.

Coordination between different emergency and government services and with media organisations is important to avoid conflicting messages and ensure that key information is widely disseminated. Dissemination of corrections and end-of-alert announcements should be improved.

The study of social media at scale and in close to real time remains in its infancy. More advanced methods, tools and shared protocols for “big data” research, as well as appropriate research training, are urgently needed, and require further funding and institutional support. In particular, a more robust infrastructure for capturing, storing, processing, and visualising very large social

media datasets is necessary. This matter also carries implications for fundamental citizens' rights, freedom of expression and data privacy issues.

6.2.6 Training schemes for technology use including new social network technologies

Accounting for technologies half-life, learning material has to be available all along. Future security research will have to provide results for uptake also on the level of dedicated training material in the context of online education, or advanced distributed learning. Research should also cover characteristics of such training materials, and the management of digital content. This should include addressing the use of new social network technologies. New social networks can provide a platform for knowledge exchange and preservation. A hierarchy of obligations-to-respond will probably be necessary for experts to differentiate between urgent/non-urgent and genuine/fake requests from social-network users. Clear rules or intelligent software are required that can prioritise the requests raised in social networks. This aspect is also of relevance for future *comprehensive approaches* to emergency management and civil protection responsive to citizens and victims needs communicated through new media channels.

6.3 OVERCOMING PRESENT AND FUTURE WEAKNESSES IN COMPREHENSIVE CRISIS MANAGEMENT

Within the work towards this deliverable, FOCUS partner Czech University in Praha (CVUT) analyzed strengths and weaknesses of the scientific and technological position of Member State and EU-level crisis management, with involvement of end-users from the civil protection sector. CVUT concluded that future EU security research should contribute to preparing rules for processing and implementing a suitable concept leading to security of both the Member State and the Union as a whole. Future security research should also propose ways to manage specific factors, vulnerabilities, risks and possibilities to common aims: the security and development of the EU as a Union.

To overcome present and future weaknesses, as anticipated by FOCUS scenario foresight, any concept for a "*comprehensive approach 2035*" should address the following aspects:

1. Introduction to problems of safety, security and sustainable development
2. Present cognition of problems of safety, security and sustainable development and set of findings on the EU management
 - 2.1 Historical concepts and experiences
 - 2.2 Management tools
 - 2.2.1 Co-ordination and responsibility matrixes
 - 2.2.2 Fundamental functions of the EU, Member States, regional and local governments
 - 2.2.2.1 Public affairs management
 - 2.2.2.2 Private organisation affairs management
 - 2.2.2.2.1 Citizen education
 - 2.2.2.2.2 Specific education of technical and managerial workers
 - 2.2.2.2.3 Technical, health, environmental, cyber and other standards, norms and rules
 - 2.2.2.2.4 Inspections and audits
 - 2.2.2.2.5 Executive units for emergency situations coping
 - 2.2.2.2.6 Systems for coping the emergency and critical situations
 - 2.2.2.2.7 Security, emergency, continuity and crisis planning

- 2.2.2.2.8 Research and development
- 2.2.2.2.9 Science on safety and on human system security
- 2.2.3 Safety management
 - 2.2.3.1 Security
 - 2.2.3.2 Sustainable development
- 2.2.4 Levels of safety management
- 2.2.5 Data, information and knowledge
- 2.2.6 Decision-making
 - 2.2.6.1 Phases, types and methods of decision-making
 - 2.2.6.2 Decision-making on public assets/affairs
 - 2.2.6.3 Rules for decision-making and decision support systems
- 2.2.7 Safety management system
- 2.2.8 Programme to increase safety
- 2.2.9 Golden rules for safety management
- 2.2.10 Groundwork for application of process management at safety management
- 2.3 Strategy and strategic management

- 3 Terms

- 4 Human system assets
 - 4.1 Basic assets
 - 4.2 Human system characteristic
 - 4.3 Conclusions for safety management

- 5 Disasters, emergencies and connections linked with management
 - 5.1 Disasters
 - 5.1.1 Disasters causes
 - 5.1.2 Disaster types
 - 5.1.3 Disaster size
 - 5.1.4 Disaster characteristics
 - 5.1.5 Summary of general findings on disasters
 - 5.1.6 Impact of disasters on human system
 - 5.2 Emergencies
 - 5.2.1 Emergency categories
 - 5.2.2 Emergency category characteristics
 - 5.3 Human system vulnerabilities
 - 5.4 Coping with emergencies

- 6. Trade-off with risks
 - 6.1 Problems connected with safety of assets
 - 6.2 Set of knowledge necessary for safety of assets
 - 6.3 Hazard and risk
 - 6.4 Life with risks
 - 6.4.1 Partial, integrated and integral risk
 - 6.4.2 Analysis and assessment of risks
 - 6.4.3 Methods used at analysis and assessment of risks
 - 6.4.4 Risk acceptability
 - 6.4.5 Qualified procedure for comparison of risks
 - 6.4.6 Processing risk assessment results to make them suitable for decision-making support
 - 6.4.7 Risk assessment
 - 6.5 Risk management and safety management
 - 6.5.1 Risk/security/safety engineering, system of systems safety engineering
 - 6.5.2 Risk management model
 - 6.5.3 Safety management model

- 7. Relevant subsystems of the EU, Member States, regional and local governments for safety management and their support
 - 7.1 Safety management stages
 - 7.2 Planning
 - 7.2.1 Planning demands
 - 7.2.2 Security planning
 - 7.2.2.1 Space planning
 - 7.2.2.2 Land-use planning
 - 7.2.3 Emergency, continuity and crisis planning
 - 7.2.4 Renewal planning
 - 7.3 Systems for decision support
 - 7.4 Security documentation
8. Selected aspects connected with safety and crisis management
 - 8.1 Information transfer and communication principles
 - 8.2 International co-operation
 - 8.3 Humanitarian aid
9. Legislation of the EU and the Members States for safety management, territory development and crisis management
 - 9.1 Basic legislation
 - 9.2 Crisis levels
 - 9.3 Crisis management bodies
10. Safety management system of the EU and the Member States
 - 10.1 Demands
 - 10.2 Relevant units (public administration, police, fire-fighters, army, citizens, etc.)
11. Proposal of plan for implementation of targets for security.

6.4 LIST OF EXPERTS

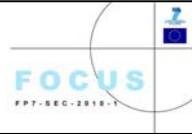
This information is not part of the public version of the deliverable.

This information is not part of the public version of the deliverable.

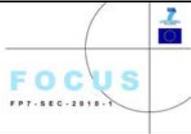
7 SUMMARY OF SCENARIO SPACE DESCRIPTION (COMMON ANALYTICAL FRAMEWORK MATRIX)

The purpose of this standard matrix is to summarise the scenario space (alternative future models for comprehensiveness and related exogenous EU roles) on the level of a common denominator for the scenarios that have emerged out of the foresight process(es). The Matrix was developed as part of the FOCUS project methodology ([Deliverable 2.1](#)). Not all categories in the matrix apply to all Big Themes.

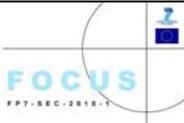
This summary will be of use for stakeholders as well as for the overall integration work in *Work Package 8*.

	<p>COMMON ANALYTICAL FRAMEWORK MATRIX</p>
<p>FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles</p>	
<p>Scenario space description</p>	
<p>Basic trends</p>	<ol style="list-style-type: none"> 1. Cooperation among Member States; 2. Multilateral cooperation by European Union in international organisations and partnerships with key actors; 3. Measures with both horizontal (involvement of law enforcement and border management authorities, with support of judicial cooperation, civil protection agencies, other sectors, and non-governmental organisations) and vertical (international, EU level, regional, etc.) dimensions. <p>Trends 2 and 3 can be summarised as bringing together all available instruments to increase EU exogenous roles, to manage interdependencies between different sectors (such as coherence of approaches of the Council of the EU and the Commission), and to coordinate actions of all stakeholders in various domains (political, structural, economic, social, etc).</p> <ol style="list-style-type: none"> 4. Growing understanding and acceptance of the comprehensive approach in addressing various security threats and challenges, with account of the interplay between those with external origin and the ones originating within the EU; 5. EU cooperation: methodology of the EU Harmony Policy Circle, which translates political priorities and threats assessments into operational action plans; 6. Economic growth in the sense of quality and capacity for innovation; 7. Coherence and inter-body relations between internal and external dimensions of security, among other things by enhancing ties between the Common Security and Defence Policy (CSDP) and Justice and Home Affairs (JHA), with focus on closer cooperation between CSDP civilian missions and JHA.
<p>Key uncertainties</p>	<ol style="list-style-type: none"> 1. EU policies with regard third countries: Will security be considered as a key factor and mechanisms for coordination between security and other related policies developed? 2. Development and management of operational instruments including, but not confined to, civil-military interaction; 3. Achievable goals and objectives in supporting non-member states; 4. Prevailing crisis management strategies; 5. Prevailing mission roles for the EU;

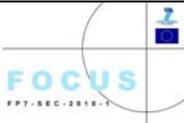
 COMMON ANALYTICAL FRAMEWORK MATRIX	
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles	
Scenario space description	
	<ol style="list-style-type: none"> 6. Geopolitical setting; 7. Development of structural conditions (e.g. consensus, subsidiarity, etc.) for effective EU decision making on crisis management; 8. Coordination, standardisation, or integration of decision-making, efforts, and capabilities, including international combination of capabilities/pooling? 9. Development of burden-sharing and division of labour between all actors involved.
Translation mechanisms: external threats and impact on societal security	<ol style="list-style-type: none"> 1. Regional conflicts out of Europe that directly and indirectly affect European interests; 2. Violent or frozen conflicts that persist on Europe's borders and threaten regional stability.
Translation mechanisms: external threats and impact on critical infrastructure	Mainly related to information and communication technology (ICT) and cyber attacks.
Major stakeholders	<i>This information is not part of the public version of the deliverable.</i>
Technology	<ol style="list-style-type: none"> 1. Development of capabilities and review of systems; 2. Definition of future operational requirements and technology development, not only in order to guarantee effective implementation of advanced concepts of operations and interoperability among military and main civilian actors, but also to lead to the creation of common civil-military assets owned by the EU; 3. Whole of community approach based on technological facilitation and empowerment, in particular new social media applications for crowd sourcing/mapping in developing operational pictures; 4. Tool for data interoperability and trusted data; 5. Network interoperability; 6. Technological solutions for interagency information exchange,
Culture/values and relevant wider societal impacts	The level of governance strongly affects the cohesion of the European Union.
Governance at EU level	<ol style="list-style-type: none"> 1. EU promotes good governance: core elements are public sector management, accountability, a legal framework for development, transparency, information, anti-corruption and the principle of participation; 2. Security sector governance (SSG) refers to the structures, processes, values, and attitudes that shape decisions about

 COMMON ANALYTICAL FRAMEWORK MATRIX	
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles	
Scenario space description	
	<p>security and their implementation. Security sector reform (SSR) aims to enhance security sector governance through the effective and efficient delivery of security under conditions of democratic oversight and control;</p> <ol style="list-style-type: none"> 3. Connection between political powers and citizens; 4. Democratic governance; 5. While security policies are increasingly involved, the main EU reference to a comprehensive approach continues to be the Common Security and Defence Policy (CSDP), which is, in turn, an integral part of the Common Foreign and Security Policy.
Governance at national level	<ol style="list-style-type: none"> 1. Connection between political powers and citizens; 2. Democratic governance.
Essential services provided to the citizens	n/a
Political Stability at EU level	n/a
Political Stability at national level	n/a
Attitude of the general public	More action at EU level against organised crime and terrorism is wanted by EU citizens.
Globalisation	<ol style="list-style-type: none"> 1. Globalisation facilitates the interconnection of threats; 2. Globalisation also implies a greater dissemination of the knowledge, which makes advanced technology easier to access; 3. Globalisation makes security depend on an effective multilateral system of international organisations, regimes, and treaties.
Regional context	<ol style="list-style-type: none"> 1. Poverty and disease give rise to pressing security concerns; 2. Security is a precondition of development. A number of countries and regions are caught in a cycle of conflict, insecurity and poverty; 3. Competition for natural resources – notably water –, which will be aggravated by global warming, is likely to create further turbulence and migratory movements in various regions; 4. Europe dependence is a special concern for Europe. It is the world's larger importer of oil and gas; 5. Regional conflicts out of Europe affect European interests directly and indirectly; violent or frozen conflicts that persist on Europe's borders, threaten regional stability.
Character/institutions of the EU	<ol style="list-style-type: none"> 1. Future of the unanimity rule fore Decisions relating to the Common Security and Defence Policy (CSDP) ; 2. Future role of the European Defence Agency (EDA) to identify operational requirements for improvement of military capabilities (possible addressing of common EU capabilities).
Interoperability and information sharing	<ol style="list-style-type: none"> 1. Whole of community approach, including contributions by individual citizens through new social media applications such as sourcing and crowd mapping; 2. Focus on people, not just systems working together: empowering citizens: training, exercising them in order to change behaviour; 3. Need for interagency information exchange policies;

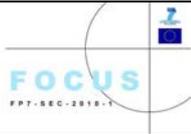
		COMMON ANALYTICAL FRAMEWORK MATRIX
FOCUS Big Theme:		
Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles		
Scenario space description		
		<ol style="list-style-type: none"> 4. Specific operational pictures based on common, accessible, understandable and trustable data; 5. Data interoperability and consistency; 6. Network interoperability, including technology-mediated new social networks; 7. Better management of data/information and utilisation of tools to develop a robust and reliable security strategy; 8. Next-generations tools: <ol style="list-style-type: none"> a. Use of visual analytics to make prioritisations; b. Trusted systems/multiple data sources; c. Checking for accuracy/authenticity of data; d. Coping with disruptive use of new social media; e. Spread of government models based on network interactions. 9. Where efficient law enforcement in the EU is facilitated through information exchange, privacy of individuals and their fundamental right to protection of personal data must be protected.
Ethical/societal challenges		<ol style="list-style-type: none"> 1. Growing influence of political and religious ideologies at the internal, neighbourhood, and global level; 2. Building trust; 3. Delivering security in a fragmented world; 4. Processing of open source data.
Main research needs		<ol style="list-style-type: none"> 1. Balanced, flexible, and effective civilian military capabilities, adequate to foreseen requirements for crisis management, peacebuilding, reconstruction and stabilisation missions; 2. Cybercrime is a global phenomenon causing significant damage to the EU internal market; 3. Comparative assessment of national policies in crisis management; 4. New technologies for collecting and integrating data from various different sources; 5. Training schemes for technology use including new social network technologies; 6. Intelligent, knowledge based focusing and filtering functions for new social media and other open information source monitoring; 7. Advancement and integration of approaches to foresight, with special consideration of: user-driven shifts, user experience as a dominant factor in technology trends, identification, and analysis of disruptors from normative end states.
New functions of security research in the scenario space	scenario planning provider	<ol style="list-style-type: none"> 1. Security research should propose ways to manage specific factors, vulnerabilities, risks and possibilities to common aims, that is the security and development of the EU as a Union; 2. The development and adaptation of legal compliance frameworks should be based on socio-demographic scenario planning. This planning should be comprehensive in that it overarches Member States' and EU levels, focusing on coordinated goal-oriented action.
	situation analyst	<ol style="list-style-type: none"> 1. Contribution to common pictures across land, shore, ship and satellite-based platforms to create situational awareness along all the EU's external borders; 2. Contribution to integrated situational pictures, networked operation command structures, and other related terminology are derived from the military domain and result from legal framework agreement between Member States.

		<h3>COMMON ANALYTICAL FRAMEWORK MATRIX</h3>
<p>FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles</p>		
<p>Scenario space description</p>		
	threat detector	<ol style="list-style-type: none"> 1. New social media monitoring tools; 2. Interfaces between human and technology-based monitoring. 3. Data integration: the extent to which standardisation of gathering and structuring of, as well as access to, information is used across multiple organisations or sub-units of the same organisation.
	securitizing actor	<ol style="list-style-type: none"> 1. Development of criteria/routines to decide whether a subject, challenge etc. falls under security or not; 2. Development of criteria/routines to decide whether research and policy strategies and resources are available to credibly and efficiently address it as such a “security” issue.
	-decision support system -legitimacy provider -provider of technical criticism	<ol style="list-style-type: none"> 1. IT-based knowledge management platforms that allow for both strategic and mission scenario planning; 2. Semantic data integration.
	awareness builder	Research-based policies at the highest possible level to make use of information in social networks, to improve external communications and outreach, to raise situational awareness and for practical operational use.
<p>New functions of security research in the scenario space</p>	<p>supporting exogenous EU roles</p>	<p>Indicative emergent research themes related to foreseen EU roles include, among others:</p> <ol style="list-style-type: none"> 1. Addressing of implementation challenges by the development of indicators for a net assessment of the effects of a comprehensive approach. This should include “societal indicators” such as election turnout, crime rates, but also arms control level, etc.; 2. Dependency on information and communication technology, and technology in general (address cascading breakdown of systems); 3. New methodologies for collecting and integrating data from various different sources; 4. Integrated situational pictures as facilitation for networked operation command structures; 5. Information exchange among civilian and military actors in order to provide common, timely and relevant situational awareness; 6. Decision-making tools based on joined-up situation analyses, including their use to secure public acceptance and support; 7. Standardised skills development and integrated information systems for a effective coordination of resources as well as to cooperation between EU Member States.
	<p>impact on internal EU roles</p>	To address alternative futures models of comprehensiveness requires, among other aspects, consideration of the security-safety continuum. In the context of the comprehensive approach, the concept of internal security cannot exist without an external dimension, since internal security increasingly depends on external security.
<p>Scenario variety</p>		<p>The scenarios developed in this deliverable project non-normative alternative paths for future developments. This means that the scenarios do not reflect desired or undesired end-states but are based on a value free analysis.</p> <ol style="list-style-type: none"> 1. Conceptual trend scenario: <ol style="list-style-type: none"> a. Concentration on “cross-sector,” “all-hazards” by wide range of measures and a strong focus on prevention, at the same time accounting for international actors and strategies and for Member State policies;

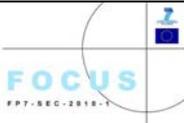
	<h2>COMMON ANALYTICAL FRAMEWORK MATRIX</h2>
<p>FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles</p>	
<p>Scenario space description</p>	
	<ul style="list-style-type: none"> b. Structured EU-wide process of development of military and civilian capabilities. 2. Policy strategies consensus scenario: <ul style="list-style-type: none"> a. Coordination between autonomous actors; b. Division of labour between all actors involved; c. International combination of capabilities/ pooling; d. Integrated assessment, decision making (systemic approach); e. Intervention-based approach (top-down/transfer of solutions, as opposed to bottom-up); f. Security strategies and policies on the EU and national levels cover the security-safety continuum. 3. Policy strategies leftovers/expert expectations scenarios: <ul style="list-style-type: none"> a. Resilience/ownership; b. Review of systems (overarching state of analysis of currently used systems); c. Common operational picture; d. Internal-external threat/security continuum; e. Knowledge/anticipation/foresight. 4. Young academics/new generation scenario: <ul style="list-style-type: none"> a. Interacting policies; b. Integrated decision making, based on integrated situational pictures and information sharing; c. Holistic approach to skills development, use of capabilities, and public acceptance; d. Citizen resilience. 5. Multinationalism scenario: <ul style="list-style-type: none"> a. Comprehensiveness as a menu of choice characterised by adaptation to reality (in terms of issues addressed, strategic objectives followed and capabilities developed and used); b. Assets, such as satellite based surveillance and communications, and cyber security capabilities that, by design, are shared by civilian and military actors and evolve from public private cooperation, which makes it difficult to reach case-by-case consensus on their use. 6. Materialism scenario: <ul style="list-style-type: none"> a. Common practice of comprehensiveness without much strategic vision, determined by temporarily prevalent; concepts for civil military cooperation (operational level), and available/usable capabilities; b. Availability of mixed civil military capabilities, based on common requirements definition; c. Full implementation of the solidarity clause. 7. Goal vs. ambition scenario: <ul style="list-style-type: none"> a. Protracted state of tension between comprehensive approach as a common strategic goal and actual levels of ambition of the EU and its Member States; b. Limited implementation of strategies and capabilities for interagency coordination and present models for civil-military interaction; c. International partnership agreements in place, but no often in practice. 8. Field experts scenario:

 COMMON ANALYTICAL FRAMEWORK MATRIX		
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles		
Scenario space description		
	<ul style="list-style-type: none"> a. Realisation of indivisible and comprehensive security; b. Based on various kinds of resources, including financial, capital, social and cultural, military and civilian capabilities as well as info technologies; c. Continuous interaction between all actors and stakeholders, including citizens. 	
Relevant results	<p>Conceptual baseline:</p> <ol style="list-style-type: none"> 1. Reflecting the cross-border and cross-sector nature of current security threats and challenges as well as the complexity of instruments and objectives in security policy along the internal-external continuum, the comprehensive approach focuses on the holistic nature and broad trade-offs involving societal goals in order to increase the security of the EU and its citizenry as a whole. 2. It aims to find and implement overarching solutions to problems, with broad effects and based on complementarity of actors, while considering all available options and capabilities, as well as the normative end-state of the security of society as a whole. 3. A comprehensive approach also entails the tackling of cross-cutting issues in home affairs. 	
Defined threats	Link to external missions	<ol style="list-style-type: none"> 1. Aggression against national territory or violation of sovereignty; 2. Proliferation of weapons of mass destruction; 3. Technology, in particular cyber attacks and attacks against telecommunication and information systems; 4. Interruption of basic resource supply chains (mainly energy); 5. Organised crime, including piracy and trafficking of drugs and weapons; 6. Illegal immigration and human trafficking; 7. Natural disasters; 8. Social or political crisis; 9. Globalisation; 10. Climate change; 11. Policy threats; 12. Health crisis; 13. Terrorism as a strategy of action and political influence; 14. War or heavy political crisis in EU neighbouring countries.
	Link to internal security	<ol style="list-style-type: none"> 1. Proliferation of weapons of mass destruction; 2. Technology, in particular cyber attacks and attacks against telecommunication and information systems; 3. Interruption of basic resource supply chains (mainly energy); 4. Organised crime, including piracy and trafficking of drugs and weapons; 5. Natural disasters; 6. Social or political crisis; 7. Health crisis; 8. Political and/or religious radicalism; 9. Terrorism as a strategy of action and political influence; 10. EU cohesion.
Input for development of the security research roadmap	<p>List of tracks for future security research, mainly:</p> <ol style="list-style-type: none"> 1. EU cohesion, decision making and governance; 2. Investment in preparedness; 3. Knowledge-based monitoring of new social media and other open 	

		COMMON ANALYTICAL FRAMEWORK MATRIX
FOCUS Big Theme:		
Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles		
Scenario space description		
		<p>information sources;</p> <ol style="list-style-type: none"> 4. Integrated situational pictures as facilitation for networked operation and command structures; 5. Information exchange; 6. Standardised skills and integrated information systems for effective coordination; 7. Training schemes for use of technology, including new social network technologies.
Used methodologies	Scenario funnel	Construction of scenario space.
	Expert workshop	Scenario development.
	Questionnaire work	<p>Scenario development</p> <ul style="list-style-type: none"> – FOCUS general expert questionnaire – FOCUS expert questionnaire “comprehensive approach <p>Both questionnaires were multiply applied in different settings</p>
	Content analysis	Scenario development and frame of reference for alternative conceptual futures of the <i>comprehensive approach</i> .
Identified future EU roles		<ol style="list-style-type: none"> 1. It is difficult to foresee exactly what exogenous roles the EU is going to assume in terms of partnerships, missions, capabilities, and challenges addressed. to an important part, future roles are expected to be shaped by the evolution of structural conditions for EU decision making. 2. Role requirements: <ol style="list-style-type: none"> a. Full recognition of the realities in a variety of countries and regions; b. Permanent screening of risk factors with technical and analytical/intelligence tools; c. Clear decision-making mechanisms at various stages of the escalation of threats and risks; d. Diverse capacities for prevention and early action against threats; e. Close communication with supporting players in the specific situation, with relevant international organisations and NGOs; f. Operational strategy based on the principle of approaching the crisis as soon as possible, as far from the Union's border as possible, as supportive/communal as possible, as peacefully as possible; g. Closer interaction of civilian and military instruments. 3. Future EU missions/operations: <ol style="list-style-type: none"> a. EU cohesion and coherence across policies; b. Governance of dissemination of knowledge and access to advanced technology; c. Governance of quality controls for nuclear installations (partial reshifting of the focus from total no proliferation to safety of nuclear technology); d. Politics of trust building. e. Political of institutions-building with a functional focus (less driven by ideas and values). 4. Policy of multilateral partnerships that rests less on EU decision making autonomy and capabilities to act.

 COMMON ANALYTICAL FRAMEWORK MATRIX	
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles	
Scenario space description	
Operational instruments	<ol style="list-style-type: none"> 1. Usable capabilities drawing from civilian and military assets; 2. Wider Petersberg Tasks; 3. Solidarity clause; 4. Possible mutual defence clause; 5. Political instruments: EU activities aimed to build political consensus on EU policy, to establish partnership relations, to intervene in international organisations or to support political or opposition authorities engaged in a conflict situation; 6. Economic instruments: policies to provide resources to achieve EU aims and to limit resources available to the opponent; 7. Intelligence instruments and information sharing; 8. Law enforcement instruments; 9. Civil protection instruments; 10. Engagement with non-profit organisations, media, and business.
Goals in supporting non-EU member states	<ol style="list-style-type: none"> 1. Promotion a ring of well-governed countries around the EU; 2. Resolution of root conflicts as a strategic priority for Europe in order to deal with other regional problems; 3. Engagement with regional partners through more effective economic, security and cultural cooperation, following to model of the Barcelona Process.
Crisis management strategies	<p>Crisis management strategies are based on the continuum of conflict and should be applied in the right time, with the right instruments, while maintaining focus of the limited use of coercion, avoidance of collateral damage of any type and the necessary consequence management.</p>
Key Drivers	<ol style="list-style-type: none"> 1. Policy drivers: <ol style="list-style-type: none"> a. EU cohesion, decision making and, more generally, governance; b. Credibility if the intended effects of comprehensiveness: willingness and capability to realise a systemic approach that integrates national and international security cultures, including human, social and political experiences, knowledge sharing, connection between national and international efforts; c. Intended societal impact of comprehensiveness: whole of community, trust building, etc.; d. Willingness to invest in preparedness; e. Politics of multilateral partnerships against global security threats; f. Policies for info exchange. 2. External challenges (and possible future key drivers): <ol style="list-style-type: none"> a. Regional/international/global distribution of wealth; b. Climate change; c. Crises resulting from scarcity of resources; d. Dependency on supply chains; e. Dependency on information and communication technology and technology in general (address cascading breakdown of systems); f. Reliability on the stability of resources (stability of providing countries); g. Convergence vs. divergence of different mind sets of different sectors, organisations, and lead actors; h. Extent of understanding of the impact that a certain

 <h2 style="text-align: center;">COMMON ANALYTICAL FRAMEWORK MATRIX</h2>		
<p>FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles</p>		
<p>Scenario space description</p>		
	<ul style="list-style-type: none"> actions is likely to have somewhere else in the system; i. Presence of sustainable leadership; j. Willingness to coordinate efforts; k. Possibility of and preparedness for exchange of sensitive information. <p>3. Technology-related challenges (and possible future key drivers):</p> <ul style="list-style-type: none"> a. Dependency on information and communication technologies (ICT); b. Whole of community approach based on technological facilitation and empowerment, in particular new social media applications for crowd sourcing/mapping in developing operational pictures; c. Technological solutions for interagency information exchange; d. Tool for data interoperability and trusted data; e. Network interoperability. 	
Validation		
Types and level of capabilities	Description	n/a
	Interoperability	<ul style="list-style-type: none"> 1. ICT-related interoperability; 2. open source intelligence applications; 3. supporting European critical infrastructure protection by technological innovation in order to guarantee interoperability between systems and data.
	Gaps (technological, norms, standards and procedures)	<ul style="list-style-type: none"> 1. Lack of definition in proceeding to achieve coordination among civil and military elements participating in operations; 2. Need for a stronger, more coherent and better integrated European crisis and disaster response capacity as well as for the implementation of existing disaster prevention policies and legislation; 3. Different national approaches definitions of criminal offences and minimum levels of criminal sanctions; 4. Lack or uniform risk management. Associated risk analysis and risk-based controls in all Member States on movement of goods across external borders; 5. (Lack of) coordination between autonomous actors, international combination of capabilities, integrated assessment and decision making, all societal outreach and transfer of knowledge; 6. Lack of comprehensive model for information exchange including a common operational picture, internal-external threat security continuum, effect-based approach to operations, resilience, effective optimisation of resources, international joining of forces, common terminology, etc.
	Technological solutions	<ul style="list-style-type: none"> 1. ICT solutions for interoperability and joined-up operations; 2. New social network technology-based tools for open information and social network analysis; 3. Online training platforms that integrate new social network

 COMMON ANALYTICAL FRAMEWORK MATRIX	
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles	
Scenario space description	
	technologies.
Interconnectedness of internal/external and civil/military security (capabilities)	<ol style="list-style-type: none"> 1. Civil-military interaction is a key driver for future conceptions of comprehensiveness; 2. Future security roles of EU will require closer interaction between civilian and military instruments to guarantee the coordination and cooperation of those involved in operations at national and international levels; 3. This interaction should be translated, in the future, into a development of military and civilian capabilities: <ol style="list-style-type: none"> a. Effective implementation of advanced concepts of operations and interoperability; b. Common civil-military assets owned in some form by the EU.
Potential for “Europeansation”	<p>Present on the fields of security economics and research into European critical infrastructure protection;</p> <p>Less or not present in the fields of public health research and security incident management research.</p>
Recommendations for courses of action	<ol style="list-style-type: none"> 1. Security research should contribute to preparing rules for processing and implementing a suitable concept leading to security of both the Member State and the Union as a whole; 2. Security research should also propose ways to manage specific factors, vulnerabilities, risks and possibilities to common aims, that is the security and development of the EU as a Union; 3. Security research should contribute to developing and implementing training schemes in particular in the following two areas: 4. Security research should have one focus on social media analysis, with case studies.
Legal and ethical guidelines for security research and innovation	<ol style="list-style-type: none"> 1. Where efficient law enforcement in the EU is facilitated through information exchange, privacy of individuals and their fundamental right to protection of personal data must be protected; 2. Transversal analysis of these aspects in the scenarios will be performed in <i>Work Package 8</i>.
Future themes for ethical parallel research in security research projects	<ol style="list-style-type: none"> 1. Effects-based approaches, international joining of forces and improvement of general political and societal acceptance at home and abroad; 2. Respect for privacy and fundamental rights to determine the requirements imposed by legislation and design constraints that assure compliance and citizens’ acceptance; 3. A more robust infrastructure for capturing, storing, processing, and visualising very large social media datasets has implications for fundamental citizens’ rights, freedom of expression and data privacy issues.
Relation of technological solutions to other components of “security preparedness”.	Human skill to deal with open source information and establish criteria to rank information for urgency, reliability, etc.

	COMMON ANALYTICAL FRAMEWORK MATRIX
FOCUS Big Theme: Alternative futures of the <i>comprehensive approach</i> and related exogenous EU roles	
Scenario space description	
Interrelations between Big Themes	Alternative futures of security research for a comprehensive approach for the EU 2035 as security provider mainly relate to the FOCUS themes of critical infrastructure and supply chain protection and disaster management.

ANNEX

DESCRIPTIONS OF THE CELLS IN THE MATRIX IN TABLE 1

This information is not part of the public version of the deliverable.