D4.5 Scenario Validation

Deliverable submitted in September, 2013 (M21) in fulfilment of the requirements of the FP7 project, ETTIS – European security trends and threats in society

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 285593.

ETTIS European security trends and threats in society	ETTIS Coordinator: Peace Research Institute Oslo (PRIO)	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.ettis-project.eu

Project Acronym	**ETTIS**
Project full title	**European security trends and threats in society**
Website	**www.ettisproject.eu** **www.ettis-project.eu**
Grant Agreement #	**285593**
Funding Scheme	**FP7-SEC-2011-1 (Collaborative Project)**
Deliverable:	**D4.4**
Title:	**Report from the Scenario Validation Workshop, including commentary and reassessment of the narrative threat scenarios**
Due date:	**31 July 2013**
Actual submission date:	
Lead contractor for this deliverable:	**Fraunhofer Institute for Systems and Innovation Research ISI**
Contact:	**Ewa Dönitz** ewa.doenitz@isi.fraunhofer.de
Dissemination Level:	**PU**

Authors:

Ewa Dönitz, Fraunhofer ISI
Erduana Shala, Fraunhofer ISI
Timo Leimbach, Fraunhofer ISI

CONTENT

FIGURES

TABLES

Executive Summary

The overarching aim of WP4 was the development of threat scenarios across different contexts in different test fields as a basis for identifying societal security needs. The selected fields, called domains, for reflecting security trends and threats are ***cyber infrastructure***, ***nuclear*** and ***environment***. Scenarios provide an in-depth analysis of the key threats. They describe the relevant future developments and offer different future perspectives for identifying future option spaces. They help to identify the main actors and their motivations by including different dimensions like society, policy, research or industry. Within the ETTIS project, scenarios serve as a base for identifying future possibilities which are solutions and options related to societal security needs.

The research work in WP4 is divided into three main parts: task 4.1 “Interviews with key stakeholders”, task 4.2 “Information mining using advanced IT tools to explore potential threats” and tasks 4.3 to 4.5 “Scenario development and identifying societal needs”. Each task delivered various inputs, e.g. future developments (trends), threats, societal security needs as well as the first ideas of solutions.

The **interviews with key stakeholders** (task 4.1, see D.4.1) provided us with input regarding current and future threats in the three mentioned domains described in D.4.4 and societal needs being also described in this report. The first insights also supported the setting of the thematic focus in each of the three domains as well as the deriving the key factors (most important aspects) for the development of the scenarios. This was an important step to prepare the scenarios. The interview partners represented conventional security research end-users as well as public and civil society organisations that are able to make statements about societal security needs at a general level. Apart from the interviews, reports and deliverables of recently completed projects with a similar focus as ETTIS were analyzed to not duplicate or reemphasize their results.

The main goal of **information mining** (task 4.2, see D.4.1) was to identify possible future threats based on a semantic internet search procedure. In addition to the interviews described above, it was the second source to identify threats. As “future threats” are a very abstract concept, it is not possible to search these threats with a simple semantic search strategy. Therefore, a two-step search strategy was developed. In the first step, a community was identified in which members of the community publish content about future threats on the internet. In the second step, the content was clustered to find out about the main topics of possible future threats and an in-depth analysis of these topics was conducted in order to receive hints about any possible weak signals for future threats. The threat identification using information mining is presented in D.4.4. The two further parts of this analysis related to the weak signals and wild cards are included in D.4.2, the methodological report within WP4.

The aim of the **scenario development** (tasks 4.3 to 4.5) was to develop the scenarios and to identify the societal security needs associated to these scenarios. This includes the analysis of already existing future studies within the domains cyber infrastructure, nuclear and environment as a preparatory step, conducting focus group workshops to gain expert opinions about the most relevant aspects in the three domains and their future development (see D.4.3) and the consistency workshop to build scenario drafts and discuss them within the consortium and with end-users (see D.4.4). The main results of these activities were the identification of threats and trends being the basis for the development of scenarios as well as a deeper understanding of the contexts of threat scenarios. The final activity described in this report was the scenario validation

workshop to identify societal security needs which are the basis for the development of solutions being dependent on scenarios.

The scenario development within WP4 proceeded at two levels: At the first level, ***four context scenarios*** were created and, at the second level, ***four threat scenarios*** for the domains cyber infrastructure, nuclear and environment were built following the principle of the context scenarios. All scenarios are described in detail in D.4.4. The terms context and threat scenarios were discussed in D3.1. The ***context scenarios*** have an overarching relevance for the field of security (e.g. EU policy, demography, trends and drivers in technology) and are equally important for the domains cyber infrastructure, nuclear and environment. The context analysis also includes the identification of emerging trends and global developments. The ***threat scenarios*** describe the most important aspects or threats in each domain and shall apply only to a particular domain (e.g. quantities regarding nuclear waste or global safety norms for dealing with nuclear material). Thus, these scenarios include threats with mostly ***procedural character*** (e.g. a lack of safety requirements or insufficiently providing information about nuclear risks). An additional analysis of threats with ***event character*** (e.g. terroristic attack or natural disaster) was conducted (see D.4.4). In order to identify ***societal security needs*** (a term also discussed in D.3.1)**,** a further analysis was carried out to investigate what happens when a threat occurs in different scenarios (see D.4.5 and the term discussion in D.3.1). The main source for the identification of societal security needs was the scenario validation workshop convened on 12 and 13 June 2013 (see chapter 1).

The scenario validation workshop delivered input to the final task (4.5) within WP4. In order to validate the outcome of the previous scenario development process, this workshop firstly contributed to the scenario discussion as well as the discussion, further identification and the selection of threats for cyber infrastructure, nuclear and environment. Secondly, it provided additional crucial and solid groundwork for identifying societal security needs which describe what happens when a threat occurs in different scenarios. The target group of the workshop was the user group encompassing the most relevant stakeholders from different security related organisations, civil society organisations, the public and researchers, high level policy-makers in the field of security as well as other stakeholders. **The presentation of the results of the validation workshop is the main purpose of this report.**

In addition to the discussions of the scenario validation workshop, further activities to identify social security needs were a part of WP4: Firstly, the interviews with stakeholders (the relevant results are presented in D.4.4) and, secondly, the analysis of security related future studies (see D.4.4 and chapter 2). The basis for this analysis were future studies relevant for the context as well as for each domain (see also D.4.4) referring to the following fields and threat sources: (i) Regardless of the domain, a broad range of different threats like the global financial crisis, the underinvestment in a critical infrastructure or the lack of human resources in the field of security was considered. (ii) There were also specific threats for each domain like wide spreading cyber IT technologies or the vulnerability of cyber infrastructure (cyber infrastructure), a lack of safety requirements by handling the disposal and the transport of nuclear material (nuclear) and biodiversity loss or urbanisation (environment). Furthermore, societal security needs were identified according to the threat scenarios. Four threat scenarios were developed for each domain based on the four context scenarios:

- The **“Common wealth”** scenario and the corresponding domain scenarios **“Good new cyber world”** (cyber infrastructure), **“Greening the image”** (nuclear) and **“Compliance with green”** (environment) are characterized by a stable political and economic framework, a competitive EU which implements security policies, a strong European

R&D landscape as well as a sinking risk awareness in society due to a peaceful surrounding.

- The scenario **“Fortress Europe”** and the corresponding domain scenarios **“Almost open”** (cyber infrastructure), **“High-security structures”** (nuclear) and **“Regulating sustainability”** (environment) refer to the global situation characterized by competing political systems, securisation and harmonisation at EU level, a stable global economy and strong security industries, trust in technology and high security as well as threat-driven R&D.
- The scenario **“Oliver-Twist-Story”** and the corresponding domain scenarios **“Going private”** (cyber infrastructure), **“Losing significance”** (nuclear) and **“Awareness without action”** (environment) describe a world characterized by shifting powers and balances in global politics and economy, a growing social gap, a minimized EU, threat- and market-driven security R&D as well as the need for security enforced by the security industry.
- The scenario **“Burying heads in the sand**” and the corresponding domain scenarios **“Fragmented world”** (cyber infrastructure), **“Losing acceptance**” (nuclear) and **“Neither awareness nor action”** (environment) are characterized by political conflicts at the global level, a growing social gap and risk acceptance, a strong security industry controlled by big players, a weak EU as well as insufficient and ineffective R&D.

The context and threat scenarios, the additional threats with event character and the first identified societal security needs resulting from the interviews in task 4.1 are described in detail in D.4.4. For this reason, **reading report D.4.4 is essential to make this validation report accessible to the reader**.

The main conclusions in this report are:

- The discussions during the validation workshop generally led to the new structure of threats in each domain and helped clarifying interdependencies between the threats. **The dynamics of the group discussions differed from group to group**: (i) The group “cyber infrastructure” invested more time in the threat discussion, in particular in structuring the threats, and delivered important implications for security needs at the general level. (ii) The groups “nuclear” and “environment” structured the threats and identified societal security needs for selected threats based on the threat scenarios.
- **There is a blurry boundary between needs and solutions** in theory as well as in project practice (interviews with stakeholders in the validation workshop). This could result from the specific nature of security being a need itself. The more specific the description of the security need is, the more difficult the distinction between need and solution is. Thus, the concrete need mostly includes solutions. Therefore, the needs stay either at a more abstract level describing issues like the need for protection or they easily end up at a level close to describing solutions like specific types of training measures or technical solutions. In principle, a higher level of description was desired in the analysis, but in some cases there were also more specific needs listed.
- **In most cases, two, three or even four scenarios showed similar patterns for each domain**. In those cases, it was hard to derive different needs. Only in some cases, it was clear that one or two scenarios strongly vary due to the different framework conditions in these scenarios. However, the impact differs between scenarios and is significantly higher or lower. Based on that assumption, the resulting needs will not vary so much in between the scenarios. There would be more differentiations possible if the likelihood would be also taken into account. **There is a diversity of societal security needs across the domains, but there are still some overlaps**:

  - Protection (e.g. of goods, immaterial goods, health, people),
  - Regulation (e.g. implementation, improvement),
  - Education, training (e.g. qualified workforce, educated society),
  - Information and transparency (e.g. about risks, measures, incidents)
  - International cooperation (e.g. regulation, agreements, enforcement),
  - Trust, reducing fear, safety culture and responsibility (e.g. trust in government, own responsibility)
  - Risk management (e.g. impact planning; simulation; modelling).
- **The scenarios are useful for analyzing how different threats impact the society** across different plausible futures described in threats scenarios. They enable the discussion of different inter-linkages between threats and needs in relation to societal, political, technological and economic issues. These results directly flow into WP5: (i) Firstly, **to evaluate what kind of solutions could be suggested** or should be developed to meet these needs in the future depending on the different framework conditions in the different scenarios; (ii) secondly, **to prioritize the solutions**: Are they robust towards the different scenarios for one domain? Are they robust towards the different domains?
- The critical review of the scenario process will be delivered in D.4.2. These findings will serve as a feedback to WP3 in order to improve the diffusion and awareness of the methodological knowledge. **The results from WP4 referring to the methodology are an important contribution to the development of an approach proposed in WP3** for the continuous monitoring and updating of threats and needs (WP4), opportunities (WP5) and priorities (WP6).

1 Approach of the scenario validation workshop and underlying data

The scenario validation workshop delivered inputs at different stages of the process: to the discussion and identification of threats and to the identification of societal security needs as well as to a deeper understanding of the developed scenarios.

In general the scenario validation workshop included structured discussion with a selected group of experts, like in this case from the field cyber infrastructure, nuclear and environment to gain information about their views to security threats and needs referred to the scenarios as well as to the further workshop aims. The interaction between the experts with different background is very important for obtaining several perspectives about the same topic. Therefore one workshop for all fields, cyber infrastructure, nuclear and environment was conducted. For this reason we invited representatives of companies which deal with security in general, e.g. work in security businesses, develop or use security technologies as well as deal with further security aspects, like societal issues.

Traditionally scenarios are built for two reasons: exploration and decision support. Scenarios explore the future and identify several future perspectives, thus provide a context in which managers can make decisions. Considering a range of possible futures, decision makers will be better informed and their decisions based on this knowledge will be more grounded and likely to succeed. Moreover, by constructing scenarios, decision makers win awareness of the variety of future possibilities, environmental uncertainties, indicators of discontinuities and the way societal processes influence one another. By developing pictures of the future decision makers already face possible events, device measurements and expand their mental models into developments not yet thought. By doing so, they prepare themselves for discontinuities in today’s world.

Scenarios cannot predict the future, but show the variety of possible futures. Thus, they are not a tool showing whether an event occurs, but a tool helping to manage its occurrence when it really happens. Therefore scenarios within ETTIS describe alternative developments as framework conditions for occurring future threats and their handling. The scenario process conducted in ETTIS relied strongly on the workshop approach. The quantitative and qualitative factors were processed alongside each other and integrated into scenarios. Building on different levels of background research, which varies in its comprehensiveness, the first important sub-step is to develop the assumptions about the future (future projections). Taking into account the basic principle of approaching the future with an open mind in the sense of “thinking the unthinkable”, a “leap into the future” is often used in the form of a workshop, which initially only concerns sketching a mentally or argumentatively imaginable world, for which the necessary sequence of steps or a roadmap are not yet known. The main steps of the scenarios process, like the development of future projections, building scenarios or identification of societal security needs, included the interaction with experts. Therefore external experts were involved in the process in order to promote the expansion of perception.

The objectives of the scenario validation workshop are embedded in the whole process of the scenario development in ETTIS (see figure 1) – the development of context and threat scenarios in step 1 as well as the additional identification of threats in step 2 (see D.4.4):

- Step 1: Development of context and threat scenarios based on the findings of the focus group workshops (see D.4.3): Research based deriving of the key factors and their future projections, focus group workshops and the survey as well as linking the context and domain scenarios using consistency analysis (consistency workshop).

- Step 2: Identifying threats additional to the creation of threat scenarios (see D.4.4): There are three sources for the identification of threats: firstly interviews in task 4.1, information mining in task 4.2 as well as focus groups and future studies analysis in task 4.3.
- Step3: Based on the results which are ***threats scenarios*** based on the ***context scenarios*** as well as the ***additional threats*** in order to identify ***societal security needs*** a further analysis was carried out to investigate, what happens when a threat occurs in different scenarios. This analysis contains the following activities:

    - Research based analysis of needs: Defining terms, structuring the existing classifications of needs, transfer of these results to the field of security, in particular to cyber infrastructure, nuclear and environment (input to WP3).
    - Threat discussion with experts: Scenario validation workshop to discuss and structure of the suggested threats as well as identifying new threats (see chapter 1.1, 1.2 and 1.3).
    - Identifying societal security needs: Scenario validation workshop to derive needs based on the threats occurring in different contexts, described by the context based threat scenarios (see chapter 1.1.2, 1.2.2, 1.3.2 and 2).

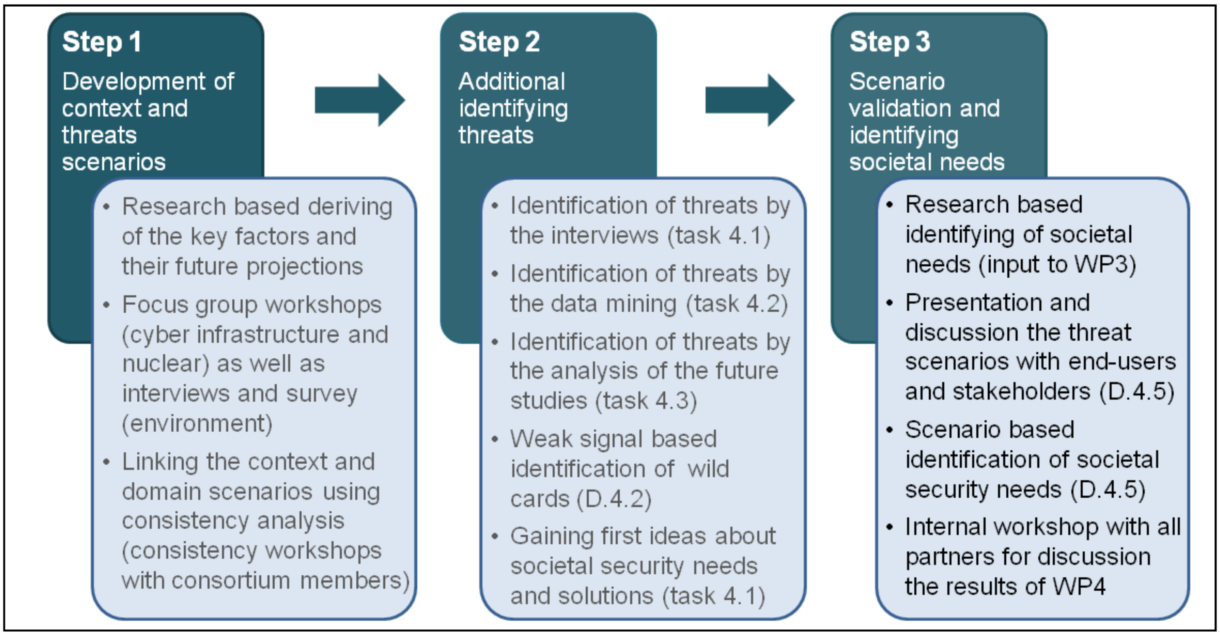
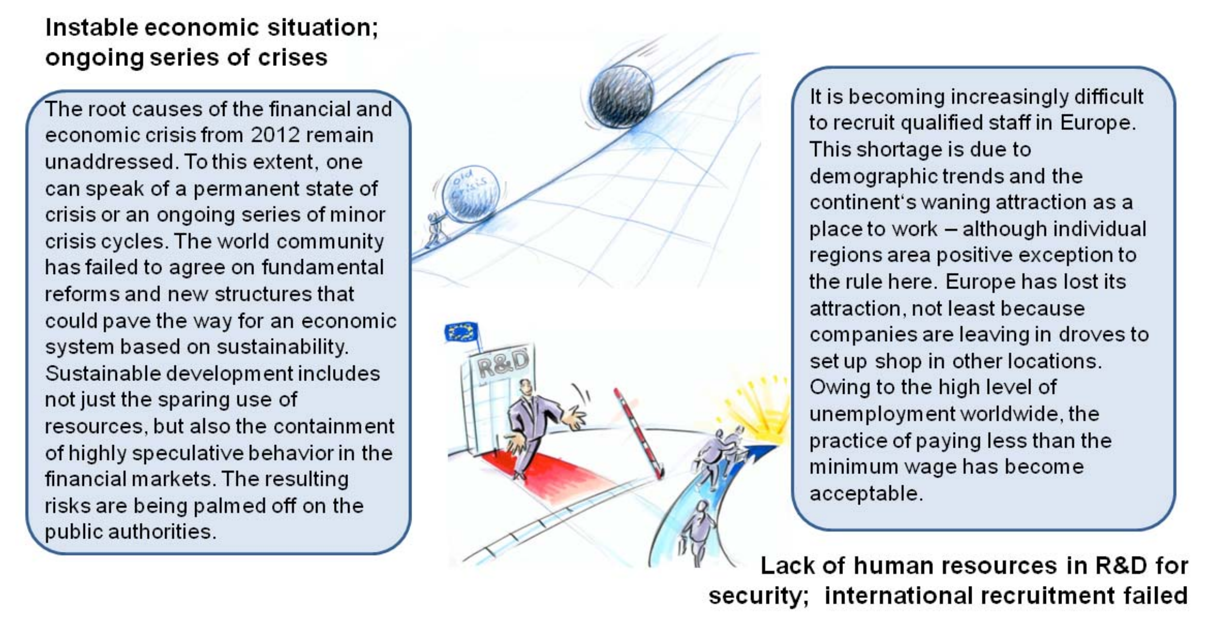

Step 1
Development of context and threats scenarios
• Research based deriving of the key factors and their future projections
• Focus group workshops (cyber infrastructure and nuclear) as well as interviews and survey (environment)
• Linking the context and domain scenarios using consistency analysis (consistency workshops with consortium members)
Step 2
Additional identifying threats
• Identification of threats by the interviews (task 4.1)
• Identification of threats by the data mining (task 4.2)
• Identification of threats by the analysis of the future studies (task 4.3)
• Weak signal based identification of wild cards (D.4.2)
• Gaining first ideas about societal security needs and solutions (task 4.1)
Step 3
Scenario validation and identifying societal needs
• Research based identifying of societal needs (input to WP3)
• Presentation and discussion the threat scenarios with end-users and stakeholders (D.4.5)
• Scenario based identification of societal security needs (D.4.5)
• Internal workshop with all partners for discussion the results of WP4

Figure 1: Three-step-process for development of the context based threat scenarios and identifying threats and societal security needs

As described above scenarios were built at two levels, context scenarios (global security scenarios) and threats scenarios (scenarios of cyber infrastructure, nuclear and environment). Thus the threat scenarios include threats with mostly procedural character (e.g. lack of safety requirements for handling nuclear material, instable economic situation or lack of human resources in R&D for security, see figure 2 and D4.4), and additional analysis of threats with event character was conducted (e.g. terroristic attack, natural disaster, see figure 3 and D.4.4).



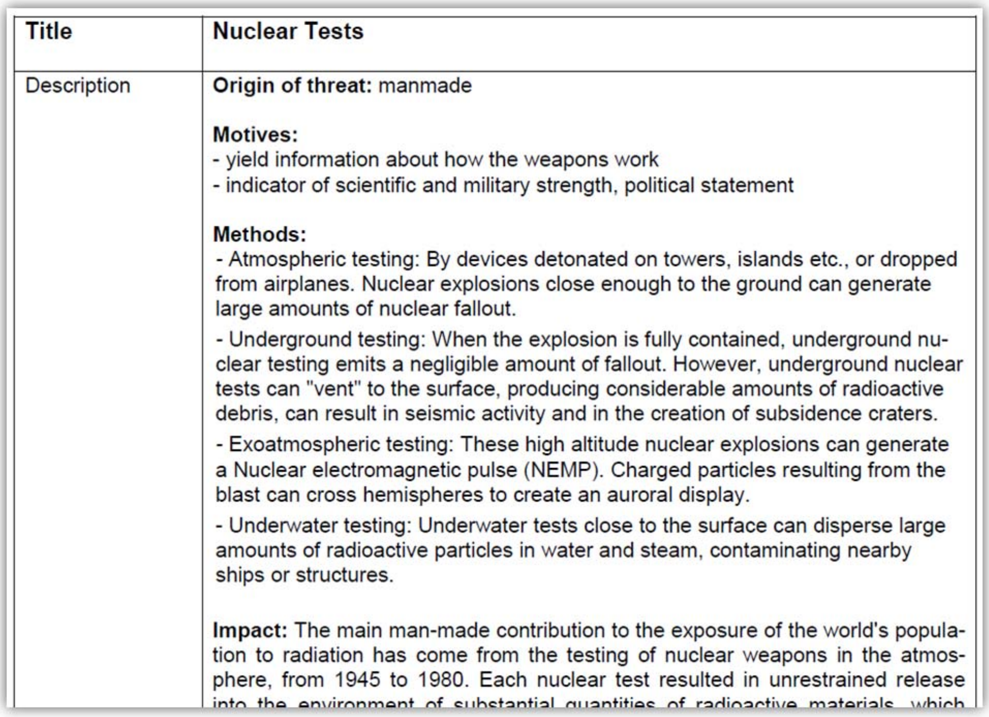
Instable economic situation; ongoing series of crises

The root causes of the financial and economic crisis from 2012 remain unaddressed. To this extent, one can speak of a permanent state of crisis or an ongoing series of minor crisis cycles. The world community has failed to agree on fundamental reforms and new structures that could pave the way for an economic system based on sustainability. Sustainable development includes not just the sparing use of resources, but also the containment of highly speculative behavior in the financial markets. The resulting risks are being palmed off on the public authorities.

It is becoming increasingly difficult to recruit qualified staff in Europe. This shortage is due to demographic trends and the continent's waning attraction as a place to work – although individual regions area positive exception to the rule here. Europe has lost its attraction, not least because companies are leaving in droves to set up shop in other locations. Owing to the high level of unemployment worldwide, the practice of paying less than the minimum wage has become acceptable.

Lack of human resources in R&D for security; international recruitment failed

Figure 2: Threats with procedural character in context based threat scenarios – an example
Illustrator: Heyko Stöber



Title	Nuclear Tests
Description	**Origin of threat:** manmade **Motives:** - yield information about how the weapons work - indicator of scientific and military strength, political statement **Methods:** - Atmospheric testing: By devices detonated on towers, islands etc., or dropped from airplanes. Nuclear explosions close enough to the ground can generate large amounts of nuclear fallout. - Underground testing: When the explosion is fully contained, underground nuclear testing emits a negligible amount of fallout. However, underground nuclear tests can "vent" to the surface, producing considerable amounts of radioactive debris, can result in seismic activity and in the creation of subsidence craters. - Exoatmospheric testing: These high altitude nuclear explosions can generate a Nuclear electromagnetic pulse (NEMP). Charged particles resulting from the blast can cross hemispheres to create an auroral display. - Underwater testing: Underwater tests close to the surface can disperse large amounts of radioactive particles in water and steam, contaminating nearby ships or structures. **Impact:** The main man-made contribution to the exposure of the world's population to radiation has come from the testing of nuclear weapons in the atmosphere, from 1945 to 1980. Each nuclear test resulted in unrestrained release into the environment of substantial quantities of radioactive materials, which

Figure 3: Threats with event character from additional analysis of threats – an example

The scenario validation workshop approach was chosen in order to support active participation and the dialogue of experts from different interested groups across and within the different domains. The discussions focused on the identification and structuring of threats and deriving societal security needs in a particular area based upon the participants' own experiences. The workshop process was a combination of different moderated activities, brainstorming as well as input presentations.

The scenario validation workshop within WP4 was a two-day event. They started with an introductory session in plenary, welcoming the participants and providing them with information concerning the project and the time schedule of the workshop. The general issues related to the project and the methodology of the workshop as well as the expectations of the hosts was discussed. In return, the participants provided information about their profession, the organisation they represent and their motivation in attending the workshop. After the introducing part the focus of the further work was on identifying, prioritising and discussing the threats and needs. The discussions have been carried out in small groups, one for each domain for cyber infrastructure, nuclear and environment, followed by the presentation of the group findings and discussion in plenary session. The workshop was finalised with a summary of the results of the workshop and a feedback from the participants in order to find out if their expectations have been met (see figure 4).

The scenario validation workshop was an important step to ensure end-user engagement throughout the scenario development. A total number of 23 participants attended the workshop, including representatives of companies, research institutes as well as the European Commission.

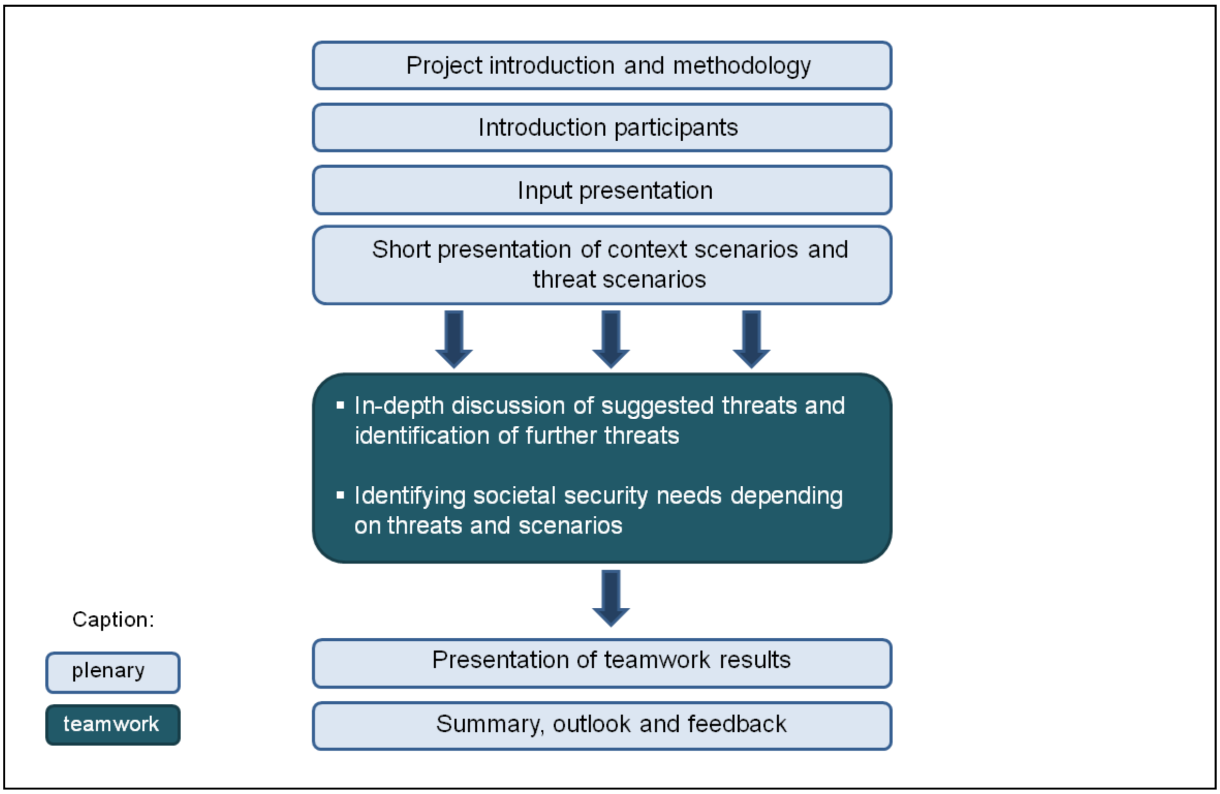

Project introduction and methodology
Introduction participants
Input presentation
Short presentation of context scenarios and threat scenarios
In-depth discussion of suggested threats and identification of further threats
Identifying societal security needs depending on threats and scenarios
Presentation of teamwork results
Summary, outlook and feedback
Caption:
plenary
teamwork

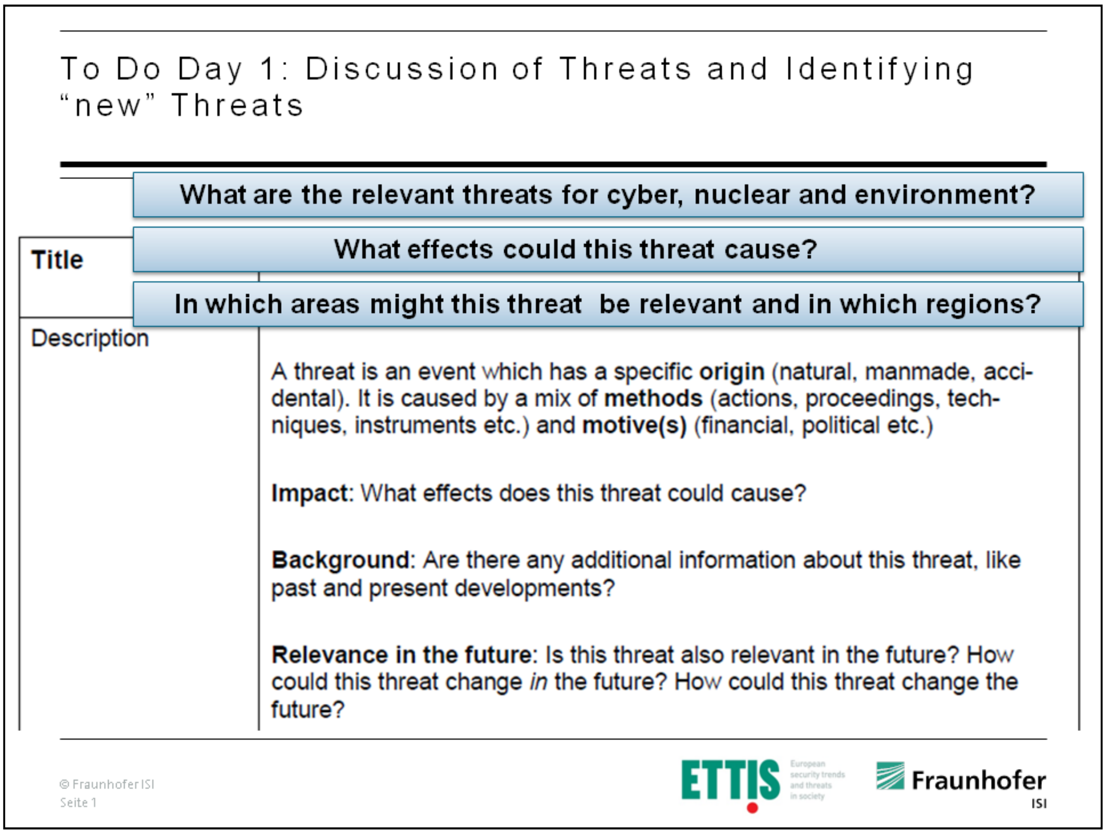
Figure 4: Schematic presentation of the scenario validation approach with WP4

The group discussions were oriented towards the following questions (see figure 5 to 7):

- What are the most relevant threats for cyber infrastructure, nuclear and environment?
- How relevant are these threats for the EU?
- What societal security needs could be derived, when a specific threat occurs in different scenarios?

The discussions led in generally to the new structure of threats in each domain and helped clarify interdependencies between the threats. **The dynamics of the group discussions differed from group to group**: (i) The group “cyber infrastructure” invested more time in the threat discussion, in particular in the structuring of threats and delivered important implications for security needs at general level (see chapter 1.1). (ii) The “nuclear” and “environment” structured the threats in the first step, followed by the identification of societal security needs for selected threats based on the threat scenarios in the second step (see chapter 1.2 and 1.3).

As a final result, the answers, opinions and recommendations were implemented in the further identification of societal needs (see chapter 2). Taking in regard the workshop recommendations the societal security needs were identified for alls scenarios as a final result of WP4 and a direct input to WP5 and 6.



To Do Day 1: Discussion of Threats and Identifying “new” Threats

What are the relevant threats for cyber, nuclear and environment?

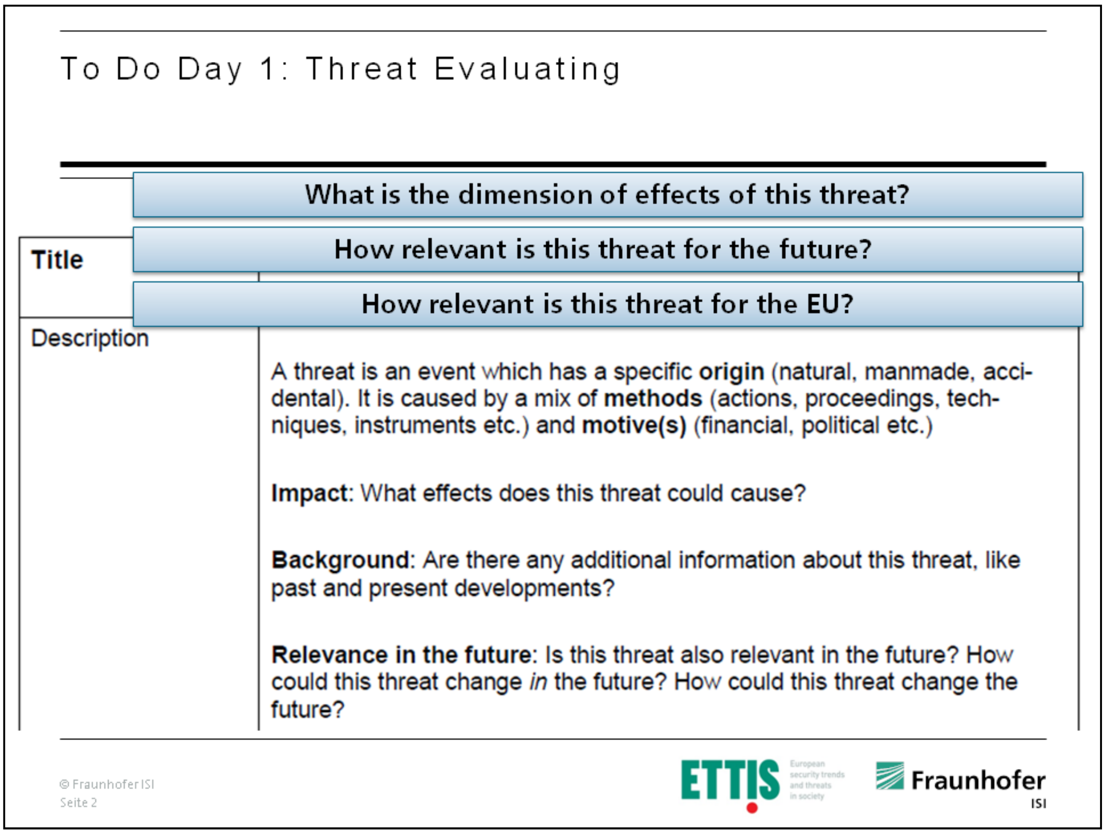
What effects could this threat cause?

In which areas might this threat be relevant and in which regions?

Title	
Description	A threat is an event which has a specific **origin** (natural, manmade, accidental). It is caused by a mix of **methods** (actions, proceedings, techniques, instruments etc.) and **motive(s)** (financial, political etc.) **Impact**: What effects does this threat could cause? **Background**: Are there any additional information about this threat, like past and present developments? **Relevance in the future**: Is this threat also relevant in the future? How could this threat change *in* the future? How could this threat change the future?

© Fraunhofer ISI
Seite 1

Figure 5: Discussion and identifying of threats



To Do Day 1: Threat Evaluating

What is the dimension of effects of this threat?

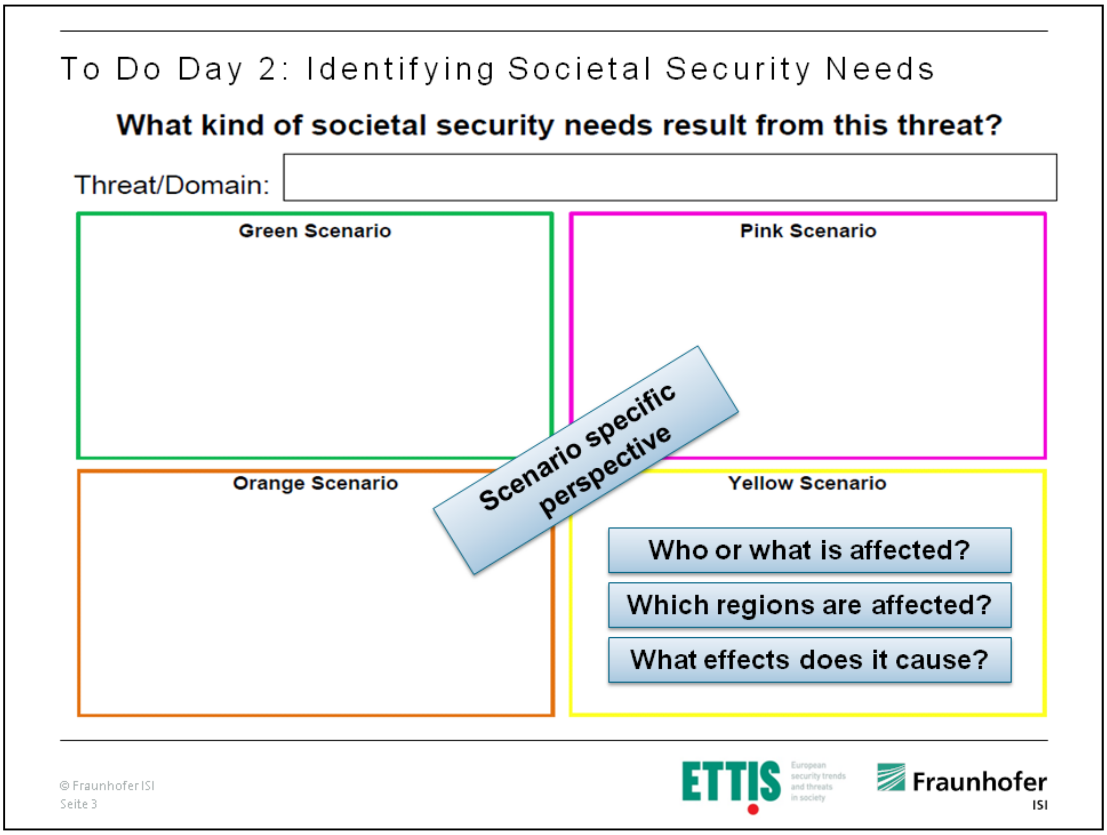
How relevant is this threat for the future?

How relevant is this threat for the EU?

Title	
Description	A threat is an event which has a specific **origin** (natural, manmade, accidental). It is caused by a mix of **methods** (actions, proceedings, techniques, instruments etc.) and **motive(s)** (financial, political etc.) **Impact**: What effects does this threat could cause? **Background**: Are there any additional information about this threat, like past and present developments? **Relevance in the future**: Is this threat also relevant in the future? How could this threat change *in* the future? How could this threat change the future?

© Fraunhofer ISI
Seite 2

Figure 6: Threat evaluating



To Do Day 2: Identifying Societal Security Needs

What kind of societal security needs result from this threat?

Threat/Domain:

Green Scenario
Pink Scenario
Orange Scenario
Yellow Scenario
Scenario specific perspective
Who or what is affected?
Which regions are affected?
What effects does it cause?

© Fraunhofer ISI
Seite 3

Figure 7: Identifying societal security needs

1.1 Findings referring to cyber infrastructure

The workshop for cyber infrastructure pursued two goals. Firstly, the list of threats should be validated and supplemented. Secondly, for each of the identified threats societal security needs should be derived. The results of it built the main input for developing the final list of threats (section 1.1.4) and a list of corresponding needs (see section 2.1), which were supplemented after workshop by additional desk research.

1.1.1 Approach of the work group

After the presentation of the main lines of development of each of the domain specific scenarios and of their main differences that was given in the plenary session, the group started with an introduction to the threats. The introduction dealt with the general challenges of developing a list of threats, including the problems of the level of abstraction, which was required; the ubiquity of ICT and its consequences like the fact that threats are often digital equivalents of non-digital threats; or the fast and often disruptive technological progress, which makes it difficult to forecast emerging threats in a longer perspective. After that the structure of the templates (see D.4.4) and the selected threats were presented in an initial overview.

After a short review of the descriptions by the participants and a first “tour de table” on impressions, a vivid discussion started. It focused on the problem of definition of the threats and the challenge to define threats for a cross-cutting, multi-purpose technology. The first point dealt with the question what are threats in the context of cyber security and how they differ from existing threats, i.e. which are really new. The second point dealt with the challenge that ICT technologies are most often used as a “tool” that helps to improve or transform existing processes in all areas of business, public administration as well as everyday life. Both points are closely interrelated and led finally to the question if there are more than the twenty already identified threats and how they could be described.

Based on that it was decided that in the second session of the group discussion a supplementing process should be undertaken that aimed at identifying further threats. This process consisted of two steps: firstly a mapping and clustering process, and secondly an analysis of results regarding important aspects like impacts, necessary framework conditions and their likelihood as well as societal security needs evolving from them.

Mapping and clustering of threats: In a first round all participants were asked to write down possible emerging threats based on their backgrounds and experiences. The results were presented and placed into a specific structure (see figure 8 below). The structure consisted of four pillars addressing the main types of activities with relevance for cyber security (criminal activities, business activities, governmental activities, consumers/citizens activities). Given the point that threats not necessarily need to be intended, but can also evolve as unintended effects of other activities, we decided to frame as: (i) threats related to criminal activities, (ii) threats related to business activities, (iii) threats related to governmental activities and (iv) threats related to consumer activities. Finally we also found, as a kind of cross-cutting, layer a set of threats that were not caused as an intended or unintended consequence of activities, but more as threats related to the organisation, technological development and structure of the system cyber infrastructure itself. After this first round of ordering, the group performed a clustering exercise, in the course of which the different threats were aggregated into clusters dealing with similar threats. The intention was to eliminate doublings and to aggregate threats so that could be used for the following threat analysis, which was completed after the workshop. The final results of this analysis, which was complemented by further research, can be found in section 1.1.4.

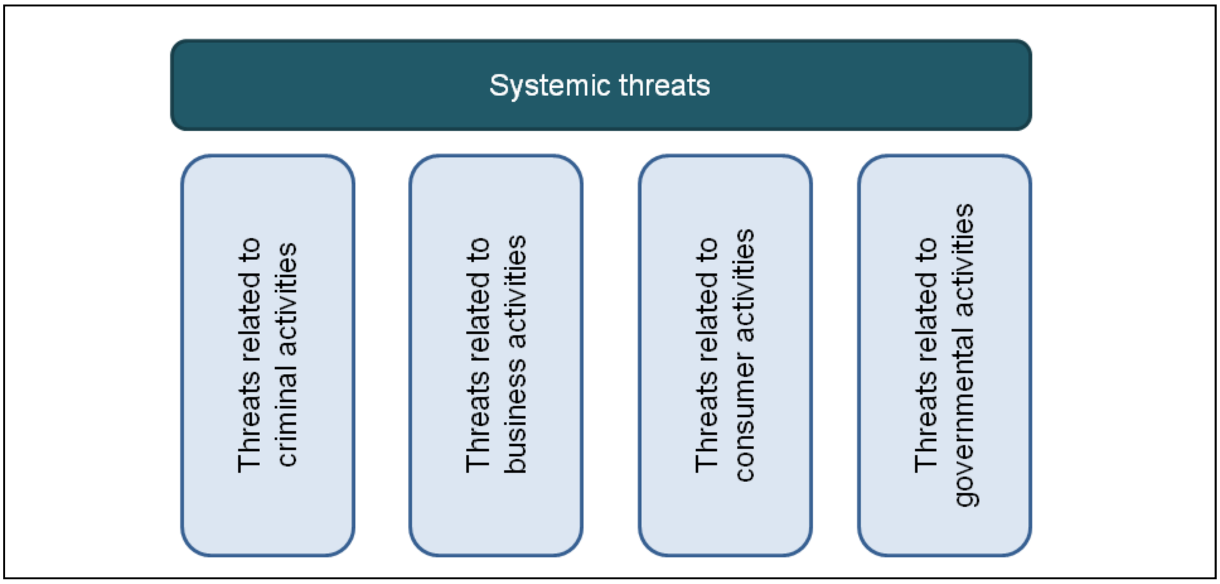

Systemic threats
Threats related to criminal activities
Threats related to business activities
Threats related to consumer activities
Threats related to governmental activities

Figure 8: Basic structure of areas for the mapping process

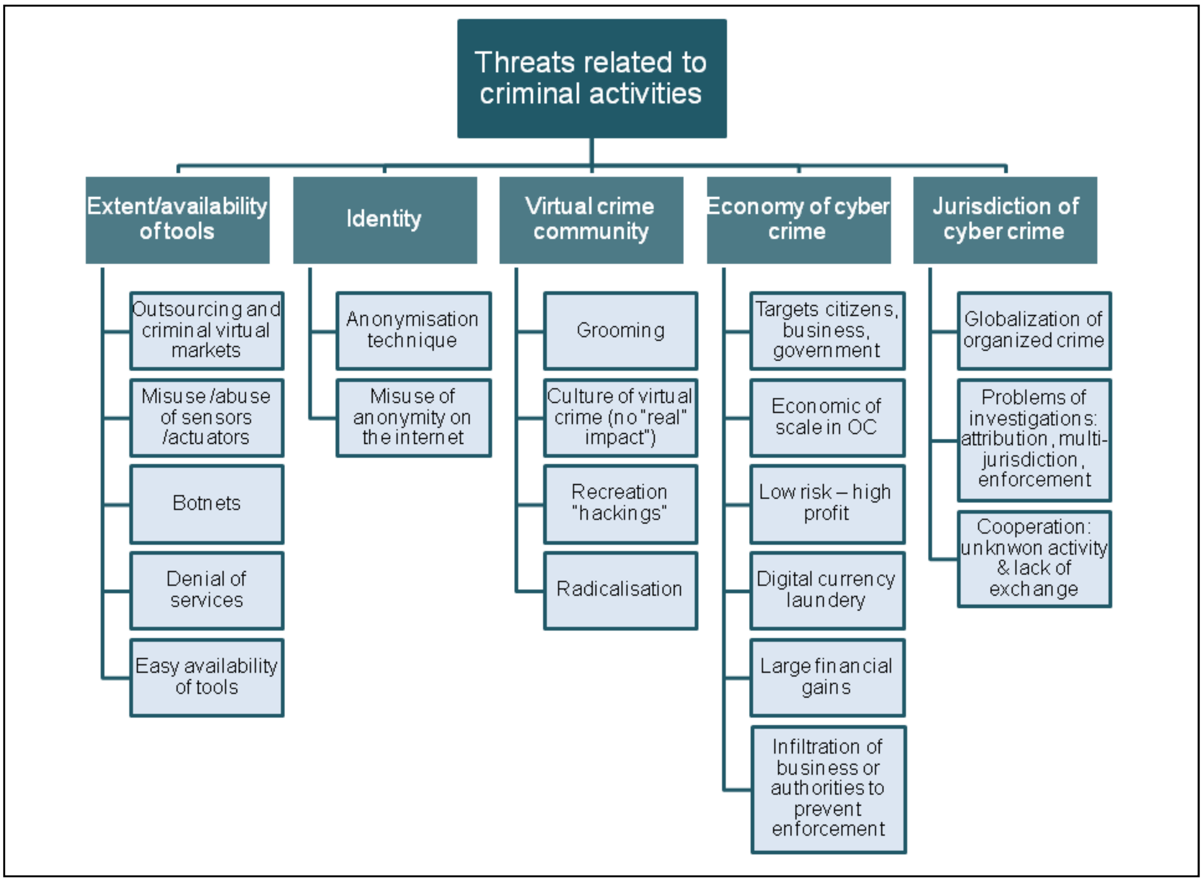
Analysis of results: This task consisted of two parts. In a first part the participants was split up into two working groups. One group dealt with the results threats related to criminal and business activities. The other group dealt with the results from threats related to consumer and governmental activities as well as systemic threats. Both groups were asked to fill out a template for each of the cluster consisting of the following points:

- short description of the threat cluster;
- future relevance;
- possible impacts (who, where, what);
- “likelihood” (including factors that influences it);
- societal relevance/impacts;
- resulting societal security needs.

The aim was to sort the identified threats and to deliver important hints for the further process of identifying societal security needs resulting from the occurrence of these threats in the different domain specific scenarios.

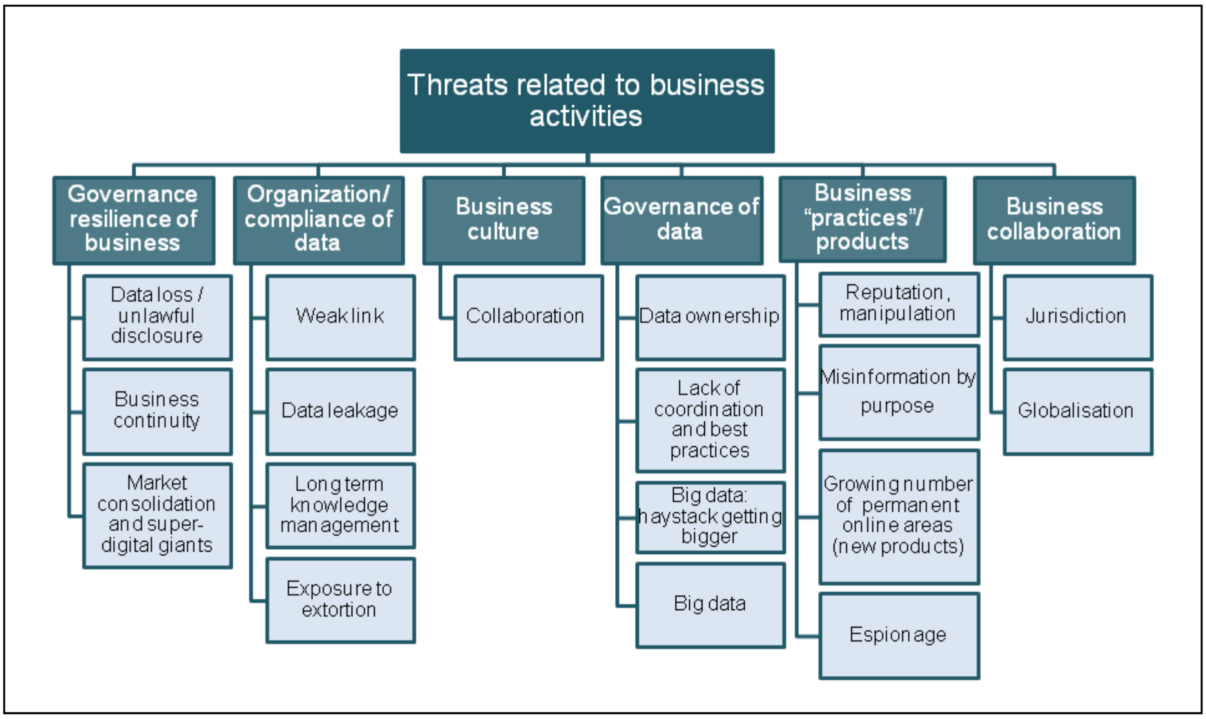
In a second step the results should be discussed and analyzed to determine how the different threats and threat cluster fit to the different scenarios and which societal security needs would arise from it. Each group gave a short presentation of the results, but given the fact that there was not enough time left to fit each new cluster into the four different scenarios, it was decided to complement the description of “likelihood” with factors that would influence the appearance and impact of the threat cluster. Based on the assessment of these factors the final matching of threats to scenarios was undertaken after the workshop taken into account information from previous workshops and desk research, which is reflected in section 2.1. Finally the remaining time was used for a discussion on the societal security needs, in particular the different problems related (see section 1.1.3).

1.1.2 Threat discussion



Threats related to criminal activities
Extent/availability of tools
Outsourcing and criminal virtual markets
Misuse /abuse of sensors /actuators
Botnets
Denial of services
Easy availability of tools
Identity
Anonymisation technique
Misuse of anonymity on the internet
Virtual crime community
Grooming
Culture of virtual crime (no "real" impact")
Recreation "hackings"
Radicalisation
Economy of cyber crime
Targets citizens, business, government
Economic of scale in OC
Low risk – high profit
Digital currency laundery
Large financial gains
Infiltration of business or authorities to prevent enforcement
Jurisdiction of cyber crime
Globalization of organized crime
Problems of investigations: attribution, multi-jurisdiction, enforcement
Cooperation: unknwon activity & lack of exchange

Figure 9: Mapping and clustering results for threats related to criminal activities



Threats related to business activities
Governance resilience of business
Data loss / unlawful disclosure
Business continuity
Market consolidation and super-digital giants
Organization/ compliance of data
Weak link
Data leakage
Long term knowledge management
Exposure to extortion
Business culture
Collaboration
Governance of data
Data ownership
Lack of coordination and best practices
Big data: haystack getting bigger
Big data
Business "practices"/ products
Reputation, manipulation
Misinformation by purpose
Growing number of permanent online areas (new products)
Espionage
Business collaboration
Jurisdiction
Globalisation

Figure 10: Mapping and clustering results for threats related to business activities

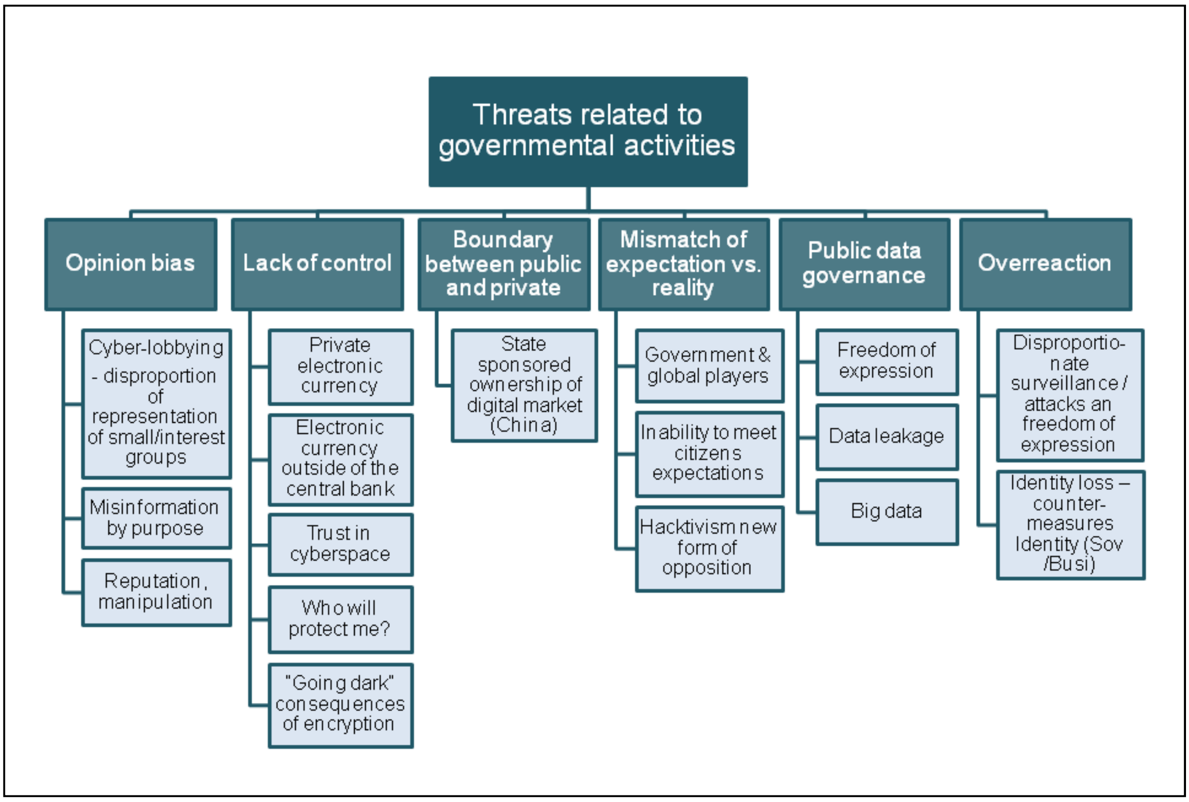

Threats related to governmental activities
Opinion bias
Cyber-lobbying - disproportion of representation of small/interest groups
Misinformation by purpose
Reputation, manipulation
Lack of control
Private electronic currency
Electronic currency outside of the central bank
Trust in cyberspace
Who will protect me?
"Going dark" consequences of encryption
Boundary between public and private
State sponsored ownership of digital market (China)
Mismatch of expectation vs. reality
Government & global players
Inability to meet citizens expectations
Hacktivism new form of opposition
Public data governance
Freedom of expression
Data leakage
Big data
Overreaction
Disproportio-nate surveillance / attacks an freedom of expression
Identity loss – counter-measures Identity (Sov /Busi)

Figure 11: Mapping and clustering results for threats related to governmental activities

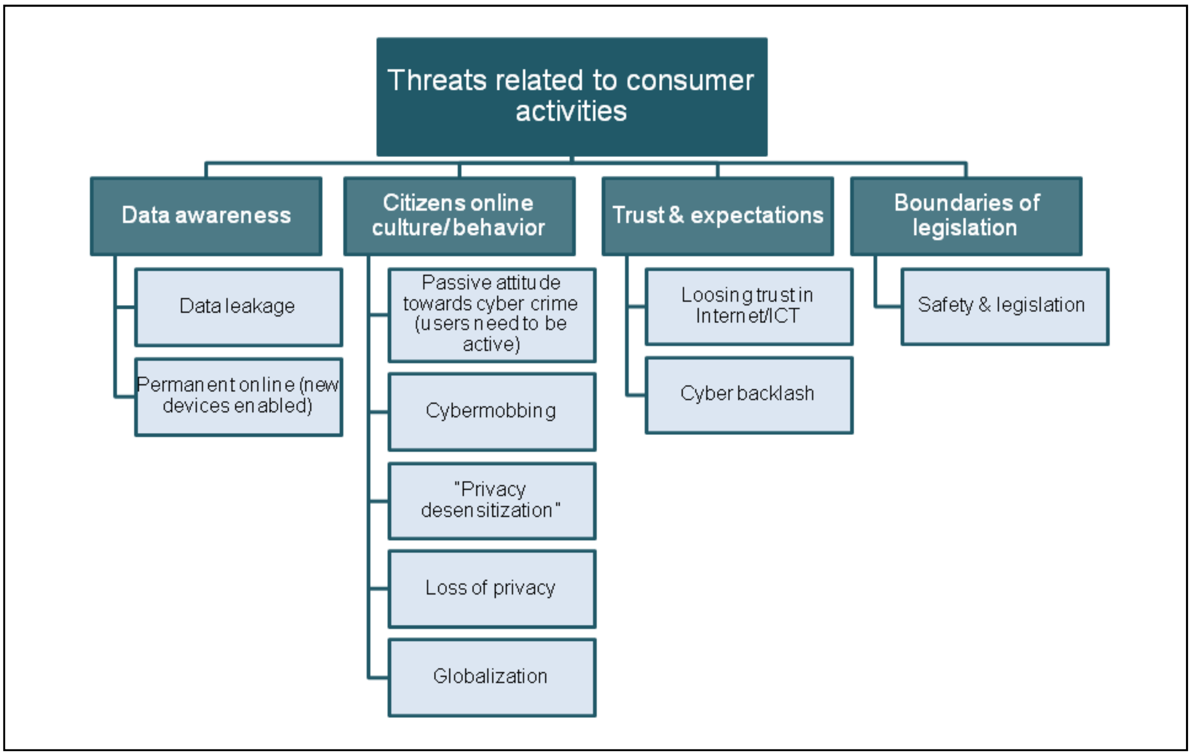

Threats related to consumer activities
Data awareness
Data leakage
Permanent online (new devices enabled)
Citizens online culture/behavior
Passive attitude towards cyber crime (users need to be active)
Cybermobbing
"Privacy desensitization"
Loss of privacy
Globalization
Trust & expectations
Loosing trust in Internet/ICT
Cyber backlash
Boundaries of legislation
Safety & legislation

Figure 12: Mapping and clustering results for threats related to consumer activities

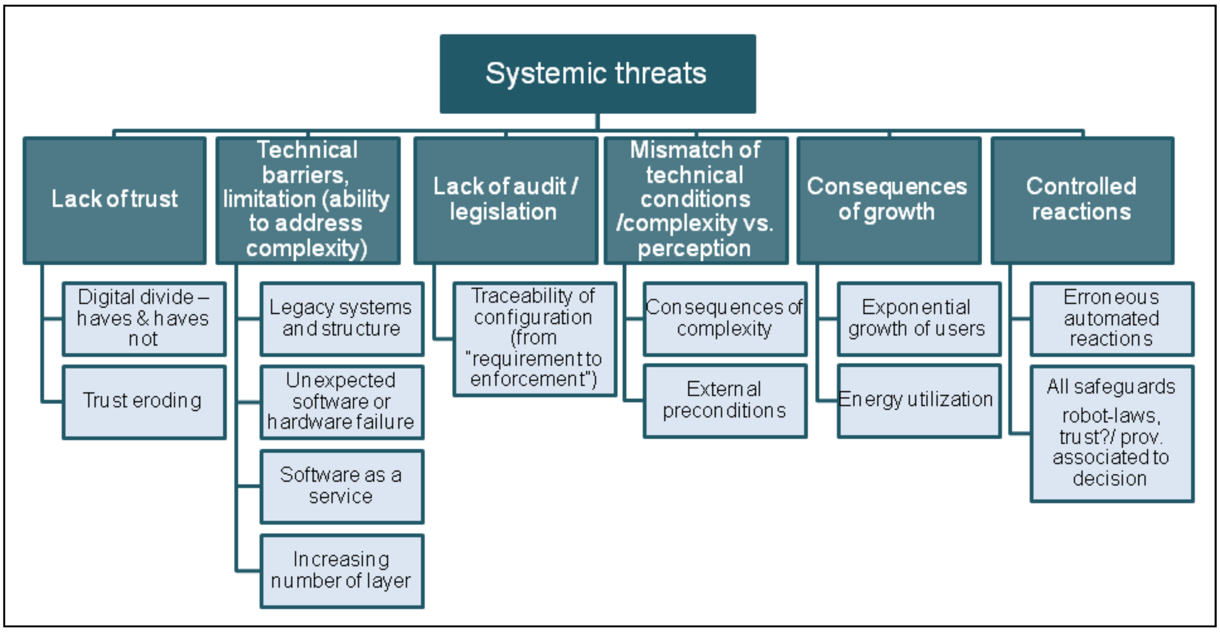

Systemic threats
Lack of trust
Digital divide – haves & haves not
Trust eroding
Technical barriers, limitation (ability to address complexity)
Legacy systems and structure
Unexpected software or hardware failure
Software as a service
Increasing number of layer
Lack of audit / legislation
Traceability of configuration (from "requirement to enforcement")
Mismatch of technical conditions /complexity vs. perception
Consequences of complexity
External preconditions
Consequences of growth
Exponential growth of users
Energy utilization
Controlled reactions
Erroneous automated reactions
All safeguards robot-laws, trust?/ prov. associated to decision

Figure 13: Mapping and clustering results for systemic threats

1.1.3 Identifying societal needs

Though the workshop was focused on validating the treats and their relations to different scenarios, one part of the work was dedicated to derive societal needs related to the identified threats. Each group was asked to name societal needs which arise from the described threat. But the initial discussion showed some difficulties related to it. The first problem was that the terming of societal needs respectively of societal security needs differed strongly between the participants. Additionally the definition of societal needs as given by the consortia (see D 3.1) was considered to be too abstract, though examples were presented. The underlying problem was twofold. One point is that security needs respectively societal needs have different meanings in the different groups, so that the results varied. The main difference was either the focus on technical aspects like “traceability of actors” and “useable solutions” or more societal aspects like “trust/confidence”. Moreover it was remarked that security itself is a societal need, where further detailing would lead to problems. This already indicates the second difficulty, the differentiation between societal needs and resulting solutions. In many cases the experts suggestions combined needs and solutions like in the case of AI safeguards, where trust building through regulation of the process (i.e. requirement of human action for critical decisions). Overall the discussion led to the questions how societal security needs can be specified and to what extend it is possible to separate needs and solutions/options during such a process of identification.

Based on this the final process of identifying the societal security needs focused on identifying overall societal needs in order to avoid the problems of differentiation described above. The results can be found in section 2.1.

1.1.4 Final list of threats

Summarizing the results of the work, the following points are obvious: (i) Firstly, as shown by the figures above some of the identified threats were identical to the existing list like for example espionage or extortion. (ii) Secondly, others had strong similarities with existing ones like cyber mobbing and the case of cyber bullying. Nevertheless the new focus often enriches the perspective of the threat. (iii) Thirdly, some of the identified threats were reflected in the future projections like complexity or technical barriers, but as shown it might be meaningful also to introduce them as specific threats. Finally the exercise and the related discussion have clearly shown the problems of identifying emerging threats, because of three points:

- The first point is that many threats in cyber often reflect existing threats, only carried out with different means. That is one consequence of the cross-cutting function of ICT technologies.
- Secondly, though they are already well-known, existing threats may change the way how they are carried out in many ways, like for example technical means, change of target groups or combination with other threats. On the one hand this underlines that "old" threats can very easily and fast become "new" threats and on the other that this may lead to different impacts and consequently different needs.
- Finally, a third point is that emerging threats often arise from an unforeseen combination of technologies, motives and possibilities, which has similarities to other developments in ICT.

Taking these results and conclusions into account the list of threats was revised and extended after the workshop. Main purpose was to combine the results of the previous work (see D 4.4) and the results of the workshop. This required some further research to differentiate the different threats and supplement them with further information. Moreover it was also necessary to adjust the results to the needs of further work packages and tasks of the project. This included aligning the level of granulation/detailing for which we decided to skip the clustering. Despite we indicate to which field each is related (1 = threats related to criminal activities, 2 = threats related to business activities, 3 = threats related to governmental activities, 4 = threats related to consumer activities, 5 0 systemic threats). This underlines that in many cases different activities respectively actors are intertwined, though we list the threats alphabetically. Instead we used the clusters as further input for new threats like the "consequences of growth", which now appear as "limits of growth". Finally 37 threats were identified:

- **"Second world" problem** – raise of alternative systems without state control, one example is the raise of electronic currencies, which are not controlled by authorities. This would minimize the control of states (3,4);
- **Accidental network breakdown** – network breakdown caused by natural forces or as consequence of unintended manmade actions (5);
- **Backslash** – people loose trust and retreat from online sphere → back to analogue worlds, which would create a new form of the "digital divide" (4);
- **Civil engagement in digital worlds** – people look way/pass by and do not engage in active commitment to help against cybercrime (passive attitude) (4);
- **Commercial cyber espionage** – targeted espionage from one competitor to the other, more targeted then governmental one (2);
- **Commercial disinformation** – manipulation of data for financial gains, for example manipulating news that could influence stock markets (1,2);
- **Commercial reputation manipulation** – manipulation of data aimed to harm the reputation of competitors, carried out by companies or criminals (1,2);
- **Criminal cyber extortion** – extortion of consumer/citizens or companies exploiting either stolen data or vulnerabilities of computer systems (1);
- **Cyber bullying/mobbing** – not only limited to young adults, but also as a problem at work or in private ("stalking"), where the digital nature makes it easy and often untraceable who was the perpetrator (4);

- **Cyber warfare –** digital warfare as a massive undertaking of one nation to harm another in many ways (3);
- **Data loss, leak and trading –** risks of leakage or loss of data, either by misuse, extortion or other ways of exploitation (1,2,3,4);
- **Data trails –** consumer use extensively new devices and services, which causes data trail which many are not aware of (4);
- **Digital currency laundry** - emerging digital currency systems, often uncontrolled by public institutions, raise the risk for uncontrolled ways of money laundry for criminals (1);
- **Digital pocket picking** - misuse of "digital wallets" like NFC credit cards, could be combination of classical pocket picking and skimming (1);
- **Digital vigilantism –** use of internet for vigilante justice, which is not legal and often hit wrong persons etc. (4);
- **Easy availability of tools –** increases the risk that more and more use it, because of high benefits and low risks;
- **Enforcement/prosecution gap** – while organized crime globalizes very quickly, jurisdiction, prosecution and enforcement are still based on national systems (1,2,3,4);
- **Global footprint –** growth of usage lead into extreme need for resources (energy, rare earth metal) (5);
- **Governmental cyber espionage** – espionage of foreign governments, business and citizens by capturing, stealing and analyzing of data, streams, activities for governmental purposes (3);
- **Governmental sabotage** – targeted sabotage by one nation to achieve specific political and/or military advantages (3);
- **Hacktivism and disproportion –** Hacktivism is an emerging form of alternative protest, which partly uses illegal methods. It often leads to disproportionate reactions of authorities up to digital surveillance enabled by the easiness of it. Overall action and reaction could lead to ongoing escalation of actions between both (3,4);
- **Identity challenges –** Identity in the net is not so clear as in real life and can be misused in different ways, either by concealing who I am, or by stealing/misusing identities of others (1,2,3,4);
- **Insider attacks** – exploitation of internal security problems by insider, which causes today most harmful attacks (in terms of damage, loss of money or reputation) on companies or public institutions (1);
- **Lack of (long term) data management** – loss of data and knowledge due to bad planning can lead to loss of important information in business (competitive advantages) or public institutions (i.e. plans for specific situations etc.) (2,3);
- **Limits of growth** – new services, new users may lead crisis of growth of the system, could be technical, organisational or others (5);
- **Monopolisation of digital business –** the risk related to the fact that a few very big, global companies dominate virtual and consequently real life (2);
- **Opinion bias** – small interest groups can gain more importance by exploiting possibilities of the internet (appear bigger as they are) (3,4);
- **Political disinformation** – the use of manipulated data to harm the reputation of politicians, parties or even whole nations on political level (3);
- **Privacy "desensitisation" –** people get used to lose privacy step by step (4);
- **Software as an institution** – more and more processes and consequently decisions are controlled only by software algorithms ("who controls the software") (5);
- **System complexity –** system of software and networks become more and more complex on both, the micro level of software (more and more lines of code) or macro level (more

and more system layers) of the system. The resulting lack of control/knowledge can lead to unexpected reactions from software and/or system (blackout, failures, etc.) (5);

- **Targeted network breakdown** – attack on the network infrastructure exploiting software or hardware flaws (1,3);
- **Terroristic sabotage** – risk of exploitation of computer flaws for terroristic actions, which is increasingly more dangerous the more infrastructure is connected (1);
- **Thievery/Burglary** – nowadays many forms of digital burglary exist, often based on identity theft, but also on deception (social engineering) (1);
- **Unclear data ownership and governance** – in times of Open Data and Big Data more and more data is available, but in many cases the ownership and consequently the responsibility for the data sets can diminish causing problems like unintended use, misinformation etc.(2,3,4);
- **Unexpected data fusion** – combination of many data sets, which may were not intended for that purpose, could lead to unexpected outcomes concerning persons (2,3,4)
- **Virtual crime communities** – while in earlier times people with certain interests had problems to find others, now new "facebook" (social networks) are created increasing risks (1).

1.2 Findings referring to nuclear

The group started with an introduction to the threats. The introduction dealt with the general challenges of threat identification, in particular the problems of the required level of abstraction, the structure of the templates (see D.4.4) as well as the content of the presented threats. After that, the group discussion focused on structuring and extending the list threats (day 1, chapter 1.2.1), followed by the presentation of the nuclear scenarios as a base for deriving societal security needs from the threats (day 2, chapter 1.2.2).

1.2.1 Threat discussion

In the first session, ten different nuclear threats were presented to the group. These were:

- nuclear espionage
- nuclear power plant accident
- nuclear proliferation
- nuclear tests
- nuclear warfare
- nuclear waste storage
- nuclear decommissioning
- nuclear material transport
- theft of nuclear material/international organized crime and illegal trafficking
- uranium mining

As an input for starting the discussion, the threats were presented in a first cluster to the group. This was arranged in three fields, of which the first was oriented on political threats like *nuclear warfare* and *nuclear tests*, the second on threats that emerge around the operation of nuclear power plants (*nuclear power plant accident, nuclear waste storage, nuclear decommissioning, nuclear material transport,* and the third on threats emerging from criminal interests, like *theft of nuclear material/ international organized crime and illegal trafficking*.

The group immediately started to investigate the source of the threats and came to the conclusion, that the threats have to be clustered in a different way because of different reasons:

- On the one hand the threats are not formulated on the same level, which means, that some of the described threats are not the threat itself but the context, in which a nuclear threat may occur. An example: *Uranium mining* is an important source for nuclear industries but not the threat itself. Yet, the damage caused to the worker's health by mining or abandoned mines occupied by unauthorized persons with criminal intent are possible threats in the context of uranium mining. The threat *uranium mining* was therefore reformulated to *front end nuclear fuel cycle causing health threats*.
- On the other hand it was noted, that different motivations in handling with nuclear material, either intentional or unintentional, may cause the same threats. An example: *Nuclear power plant accident* could be caused by human or nature.
- Further, there is a contrast between threats of high probability and low impact vs. threats of high impact and low probability. The conclusion was that the most threats are not very likely, but they have a high impact (see the explanation below).

This opened the discussion about classifying the nature of threats and how or by whom they are caused. The conclusion was that nuclear threats are caused by (1) theft, (2) attack or (3) accident (see figure 14).

Generally it was argued, that there are intentional threats and unintentional threats. Intentional threats are attacks and theft of nuclear material, whereas accidents, either caused by humans or nature, are unintentional. Each threat, when come true, has different impacts on the society. These may be ideological, psychological or may cause fear in society, which then affects the risk perception about nuclear threats in general.

Another crucial point of the discussion was that nuclear threats at some level have to be regarded as radiological threats, as they may not only occur with the same source, intent and consequences only in the nuclear sector, but also in other sectors which use radiological material, e.g. in hospitals.

A further point which was crucial for the following task on linking societal security needs to the scenarios, was the question on the probability of threats. It was argued, that most of the nuclear threats are not very likely to happen due to the high security standards in nuclear power plants. It was argued that in states where the nuclear sector has a long history, security awareness is very high as risks and threats are well known. In contrast, states with new nuclear programs mostly have a lack of the security awareness and standards and also a lack of experience, which might increase the probability of accidents. Nevertheless, the consequences of nuclear theft, attacks or accidents have a high impact due to cascading effects, independently of the location of appearance.

Taking into consideration the discussion described above, five different threat sources were identified (see figure 14):

- proliferation
- theft of nuclear/ radiological materials
- loss of nuclear/ radiological materials
- accidents at nuclear/ radiological facilities
- terrorist attacks on nuclear/ radiological facilities

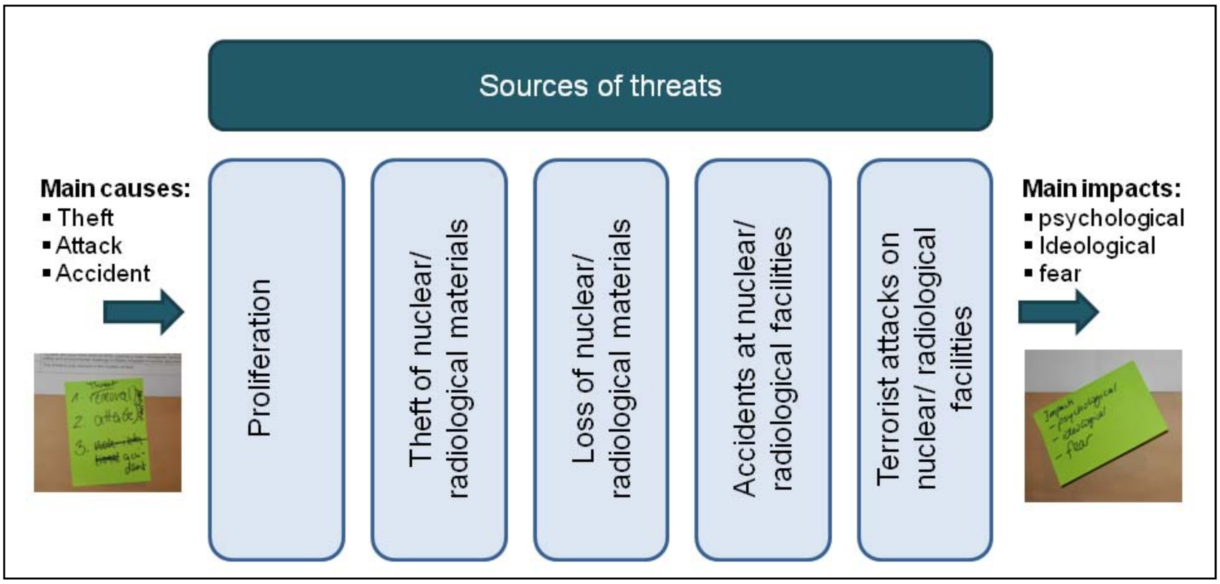


Figure 14: Five sources of nuclear threats with remarks on intent and impact of nuclear threats

The ten threats which were proposed in the beginning of the session may all be assigned to one of these five threat sources or rather are the context for one of those. The group also found some more threat examples which can be assigned to those sources:

- nuclear shutdown
- radiological threats from sources outside the nuclear industry
- low level of trust in institutions
- higher risk of nuclear accidents in countries with new nuclear programs

To complete the structuring of the threats, their sources and their implications, the group finally discussed if the threats were safety threats or security threats. This was quite helpful for the next session, as societal security needs may differ depending on whether the threat is a safety or a security issue (see figure 15):

- Accidents are a safety issue. It was defined that accidents may happen at nuclear and radiological facilities and cause radiological contamination. Examples of where and when accidents may happen are: decommissioning, transport, operation of plant, front-end fuel cycle (mining, enrichment), storage, regulatory maturity/ effectiveness or loss.
- Threats, which are a security issue, are proliferation, theft of radiological materials/ nuclear technology, loss of nuclear/ radiological material and terrorist attacks (cyber, physical).
- The group agreed on nuclear warfare to be a wildcard, which is linked to the security issue. It was argued that nuclear warfare is not a threat linked to the nuclear sector, but rather a political issue. Thus, it has a very low probability but a high impact especially on security issues, but also on safety aspects. This wildcard may also decrease the level of trust in institutions regarding the nuclear sector.

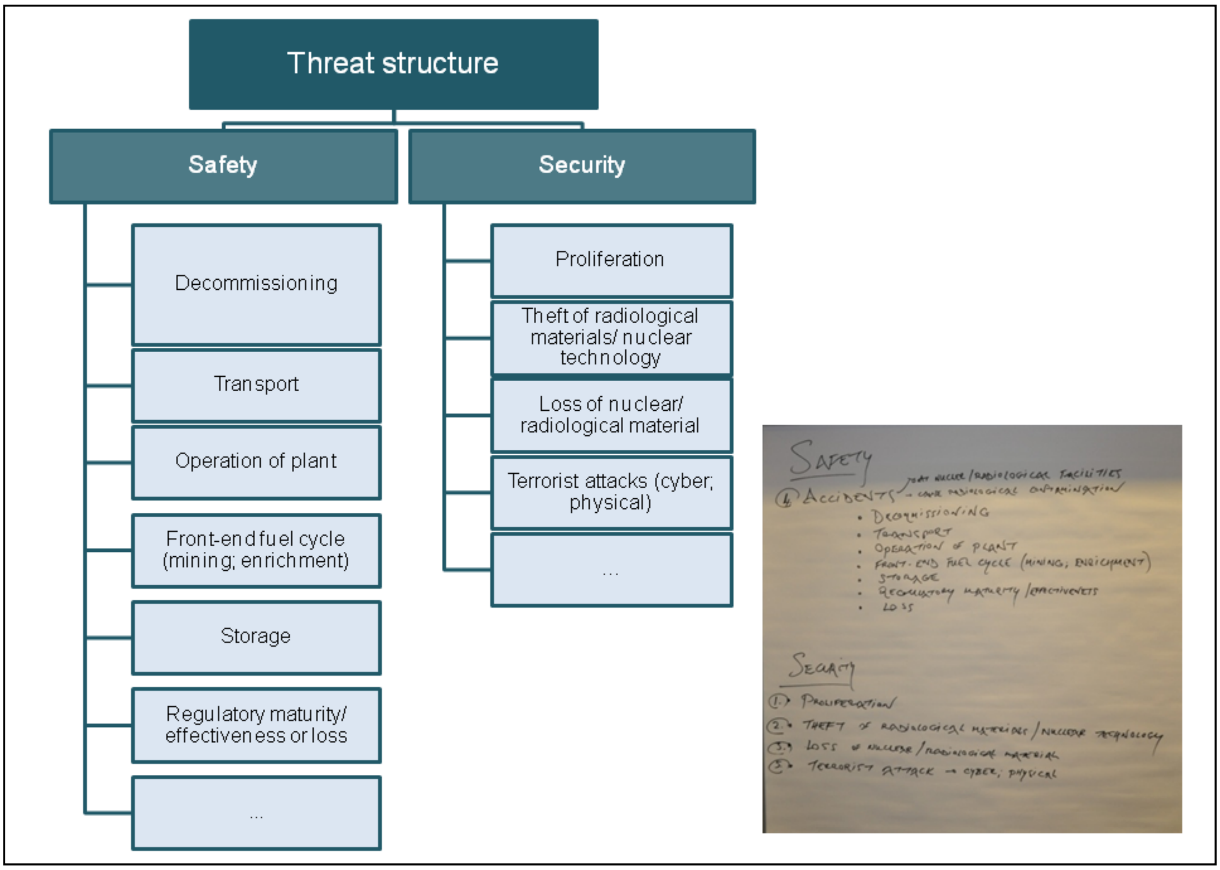

Threat structure
Safety
Decommissioning
Transport
Operation of plant
Front-end fuel cycle (mining; enrichment)
Storage
Regulatory maturity/ effectiveness or loss
...
Security
Proliferation
Theft of radiological materials/ nuclear technology
Loss of nuclear/ radiological material
Terrorist attacks (cyber; physical)
...
SAFETY
4 ACCIDENTS THAT NUCLEAR/RADIOLOGICAL FACILITIES → CAUSE RADIOLOGICAL CONTAMINATION
• DECOMMISSIONING
• TRANSPORT
• OPERATION OF PLANT
• FRONT-END FUEL CYCLE (MINING; ENRICHMENT)
• STORAGE
• REGULATORY MATURITY /EFFECTIVENESS
• LOSS
SECURITY
1. PROLIFERATION
2. THEFT OF RADIOLOGICAL MATERIALS/NUCLEAR TECHNOLOGY
3. LOSS OF NUCLEAR/RADIOLOGICAL MATERIAL
5. TERRORIST ATTACK → CYBER; PHYSICAL

Figure 15: 5 Structuring threats into safety and security issues during the workshop

The following table shows a summary of the findings of the first session.

Issue	**Threat**	**Appearance**	**Matching input threat list/ *examples of the group***
Safety	Accident	Decommissioning	Nuclear decommissioning
		Transport	Nuclear material transport
			Radiological threats from sources outside the nuclear industry
			Higher risk of nuclear accidents in countries with new nuclear programs
		Operation of plant	*Nuclear shutdown*
			Nuclear power plant accident
			Low level of trust in institutions
			Higher risk of nuclear accidents in countries with new nuclear programs
		Front-end fuel cycle (mining; enrichment)	*Front end nuclear fuel cycle causing health threats* (uranium mining)
		Storage	*Low level of trust in institutions*
			Nuclear waste storage
		Regulatory maturity/ effectiveness	*Low level of trust in institutions*
		Loss	Nuclear material transport
Security	Proliferation		Nuclear proliferation
			Nuclear espionage
			Nuclear tests
	Theft of radiological materials/ nuclear technology		Nuclear material transport
			Nuclear espionage
			Theft of nuclear material/ international organized crime and illegal trafficking
	Loss of nuclear/radiological material		Nuclear material transport
	Terrorist attacks (cyber; physical)		Nuclear espionage
			Nuclear warfare

Table 1: Findings of nuclear threat discussion – tabular summary of the first session

Taking the structuring of threats into safety and security-relatedness and appearance into account, a list of 19 threats can be derived and used for identifying societal security needs:

- Accidents while **nuclear decommissioning**
- Accidents during **nuclear material transport**
- Radiological threats from **sources outside the nuclear industry**
- Higher risk of **nuclear accidents during transport in countries with new nuclear programs**
- Accidents by **nuclear shutdown**
- **Nuclear power plant accident** during operation of plant
- **Low levels of trust in institutions** may lead to fear in society and risk of accidents
- Higher risk of **nuclear accidents in countries with new nuclear program during operation of a nuclear power plant**
- **Accidents in front end nuclear fuel cycle causing health threats** (like uranium mining)
- **Accidents in nuclear waste storage**
- Safety threats caused by **accidents** due to exceeded regulatory maturity

- **Loss of nuclear and radiological material**, e.g. during transport, causing safety and security threats
- **Nuclear proliferation** causing security threats
- Security threats due to **nuclear espionage** for proliferation
- Security threats due to **nuclear tests** for proliferation
- **Theft** of radiological materials/ nuclear technology during nuclear material **transport**
- **Theft** of radiological materials/ nuclear technology by **nuclear espionage**
- **Theft** of radiological materials/ nuclear technology due to **international organized crime and illegal trafficking**
- **Terrorist attacks** (cyber; physical), may occur by nuclear espionage

1.2.2 Identifying societal security needs

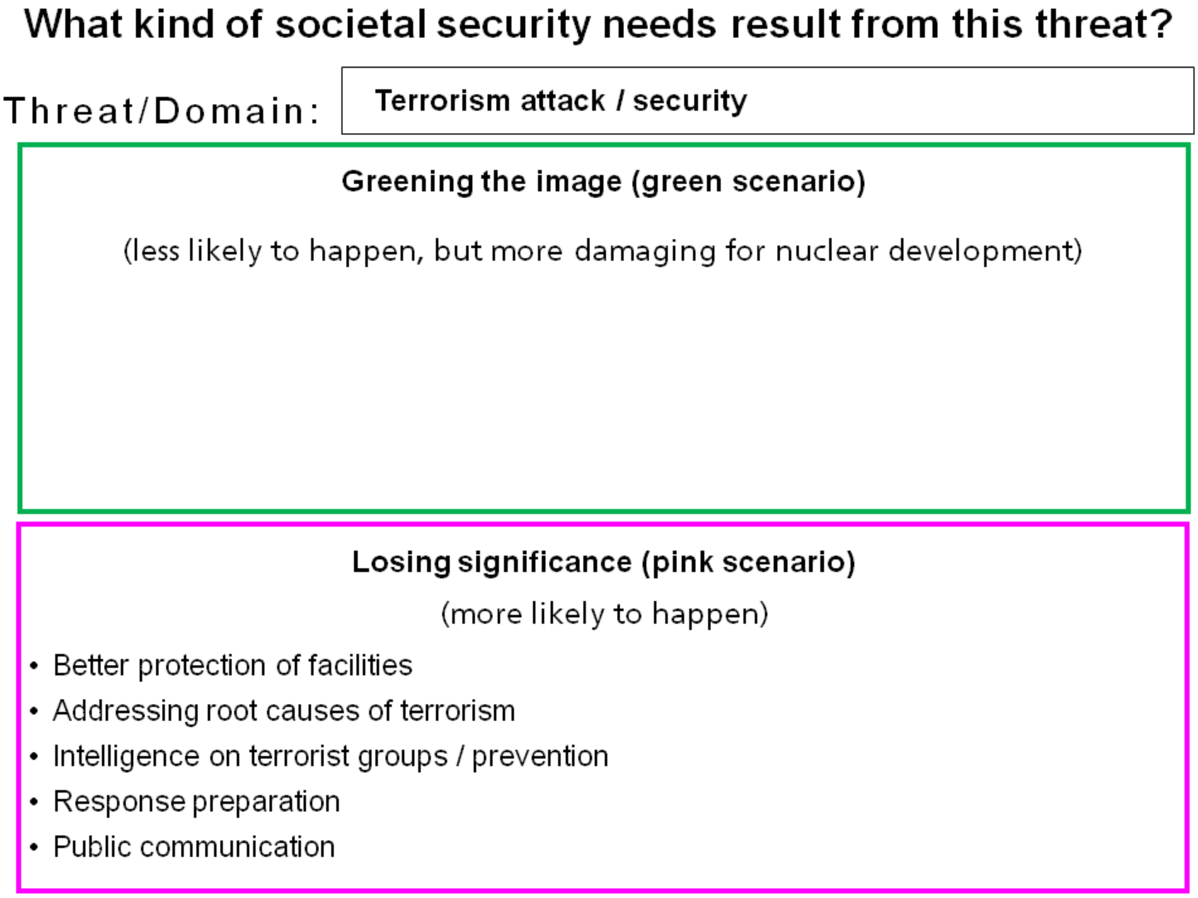
The second session which aimed at finding societal security needs started with the presentation of the four nuclear domain scenarios, in which the threats should be projected.

For identifying societal security needs, the group orientated itself on the new structure of threats, as described in the previous chapter. The group concentrated on the five identified sources of threats,

- proliferation
- theft of nuclear/ radiological materials
- loss of nuclear/ radiological materials
- accidents at nuclear/ radiological facilities
- terrorist attacks on nuclear/ radiological facilities

It was argued, that all threats which are assigned to one of these threat sources, have the same effects on societal security needs. Further, it was argued that the threats are probable in each of the four scenarios. The only difference is that some threats are more likely to happen and have a higher impact in some scenarios than in other ones. The societal security needs in regard of nuclear threats differ only slightly in the orange, the pink and the yellow scenario, whereas there are other societal security needs in the green scenario. The overview of the scenarios is presented in chapter 2 and the detailed descriptions in appendix.

Below, two different examples are shown which refer to a security threat and a safety threat (see figure 16 and 17). The group described the main differences by taking a closer look to the green and the pink scenario.



What kind of societal security needs result from this threat?

Threat/Domain: Terrorism attack / security

Greening the image (green scenario)

(less likely to happen, but more damaging for nuclear development)

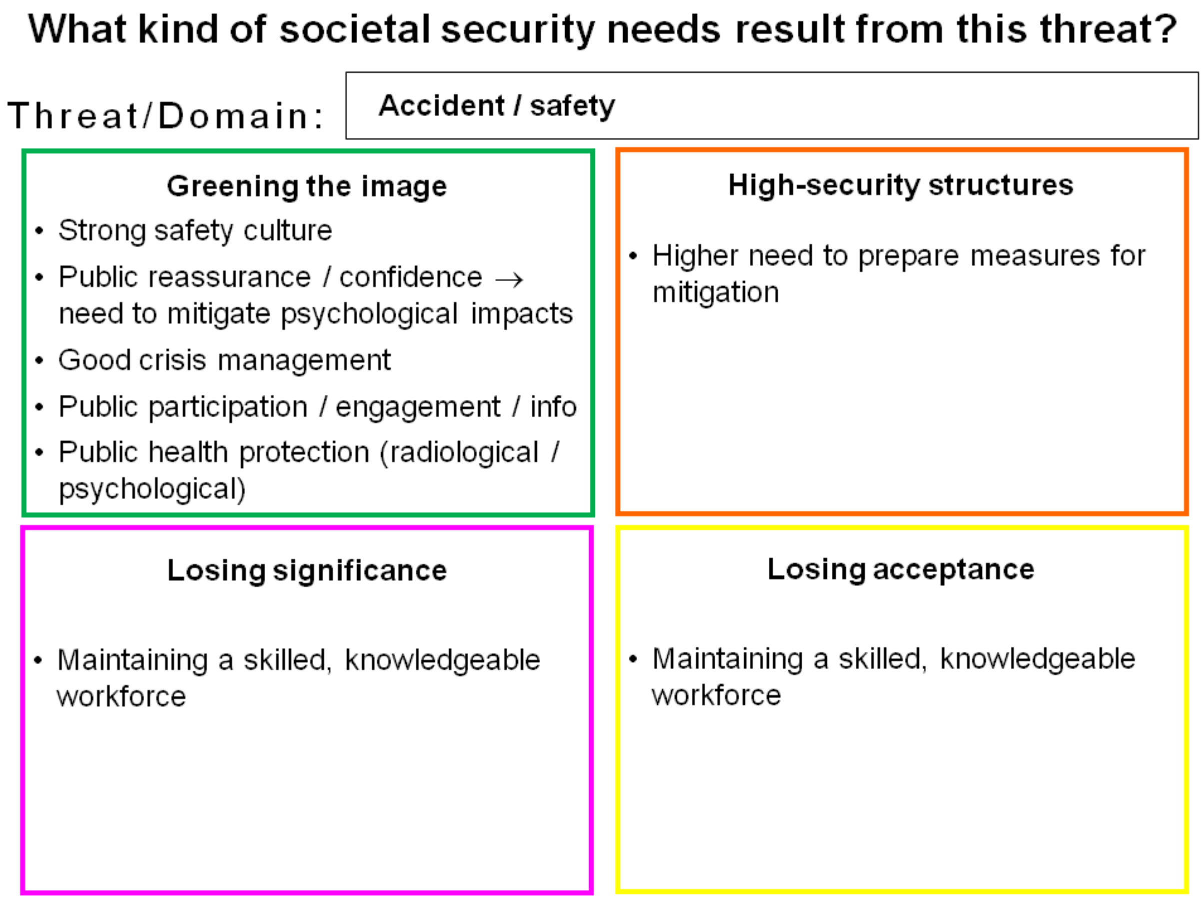
Losing significance (pink scenario)

(more likely to happen)

- Better protection of facilities
- Addressing root causes of terrorism
- Intelligence on terrorist groups / prevention
- Response preparation
- Public communication

Figure 16: Scenario-based deriving of societal security needs from the threat terrorist attack

The threat *terrorist attacks* is more likely in the pink scenario than in the green one. In case of a terrorist attack in the green scenario this event would be more damaging for the development of the nuclear sector, as it has reached a good reputation and high security measures. But in a first instance, people would hardly have societal security needs related to terrorist attacks in a peaceful world. In contrast, a terrorist attack is more likely to happen in the pink scenario as there is an instable political and economic environment. In regard of this threat societal security needs are more pressing in the pink scenario, e.g. the need for better protection of facilities, need for public communication or the need for addressing root causes of terrorism.



What kind of societal security needs result from this threat?

Threat/Domain: Accident / safety

Greening the image

- Strong safety culture
- Public reassurance / confidence → need to mitigate psychological impacts
- Good crisis management
- Public participation / engagement / info
- Public health protection (radiological / psychological)

High-security structures

- Higher need to prepare measures for mitigation

Losing significance

- Maintaining a skilled, knowledgeable workforce

Losing acceptance

- Maintaining a skilled, knowledgeable workforce

Figure 17: Scenario-based deriving of societal security needs from the threat accident
Note: Scenario green contains a mix of needs and framework conditions

In contrast to the security threat *terrorist attacks*, a safety threat like an *accident* strongly affects societal security needs in the green scenario. As there is a high share of the nuclear industry in the green scenario, there is constantly a level of safety measures to be met. It is very likely that there is a strong safety culture and a sufficient crisis management in the green scenario. But in case of an accident, there is e.g. a high need to mitigate psychological impacts. To maintain the acceptance of the technology any longer, there is also a need for public participation and informing the public about health protection. In the pink scenario, where the acceptance of the nuclear industry is not as widespread as in the green scenario, the main need is to maintain a skilled and knowledgeable workforce. The reason is that security standards may suffer in this scenario. The same needs occur in the yellow scenario. In the orange scenario, which is characterized by high security standards, there might be a higher need to prepare measures for mitigation.

1.3 Findings referring to environment

The approach of the group nuclear was also applied by the group environment:

- Firstly the threats were presented. The introduction dealt with the general challenges of threat identification, in particular the problems of the level of abstraction, which was required, the structure of the templates (see D.4.4) as well as the content of the presented threats.
- Secondly the group structured and made amendments and additions to the initial list of threats (day 1, chapter 2.2.1).

- Thirdly environment scenarios were presented in order to gain awareness of the participants as a basis for deriving of societal security needs (day 2, chapter 2.2.2).

1.3.1 Threat discussion

The following threats were presented to the group:

- Air pollution
- Water pollution
- Biodiversity loss
- Complex nexus among resources scarcity: food, water, energy & minerals
- Deterioration or loss of ecosystem services
- Crime – food fraud and food terrorism
- Plastic garbage patches as threat for food safety and security
- Greenhouse effect/ Global warming
- Growing western dependency on oil, gas and import of minerals and high tech metals
- Habitat loss and degradation – forest and coral reefs as an example
- Introduction of invasive alien species
- Loss of arable land
- "Natech" disasters (Natural disasters in combination with man-made accidents)
- Pharmaceutical residues from pharmaceutical discharges or residues of veterinary drugs
- Resource access triggered conflicts within and between states

The group immediately started to classify these threats and build different clusters. It came to the conclusion, that there are different levels of threats and there are interfaces between the suggested clusters (see figure 18). Another important insight resulted from the discussion about the nature of threats. In the opinion of the participants, environmental threats have mostly procedural character (as slow developments). Threats like natural or human caused hazards and disasters have an event character. The group came to the conclusion that in general threats could be: events (e.g. *natural hazards* or *accidents*), technologies (e.g. genetic engineering), framework conditions (e.g. lack of regulation or *crime and corruption*) and process (*urbanisation* or *soil erosion*).

Furthermore threats could be formulated at a very different level of abstraction: (i) On the one hand the definition could be very broad, e.g. *conflicts within and between states*, *crime and corruption* or *resource availability and use* (see the upper and down part of the figure 18). (ii) On the other hand threats could be also very specific, e.g. *soil erosion* (see figure 19). In the first case threats are mostly caused by other threats, thus cascading effects could arise. For example the high-level threat *food security* or *resource availability and use* might result from *habitat loss and degradation*.

The environmental threats find themselves caught between policy and economic developments and threats with many interdependencies between these fields.

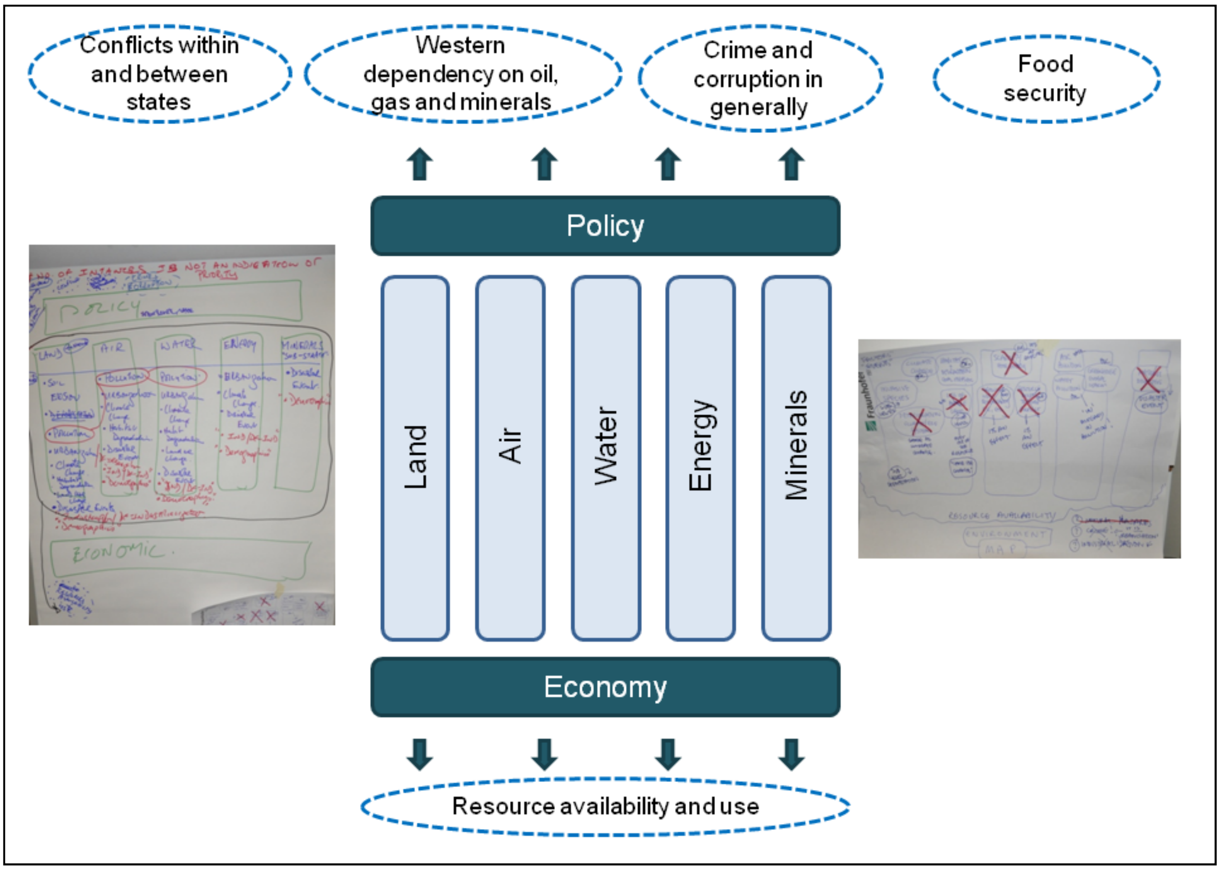

Conflicts within and between states
Western dependency on oil, gas and minerals
Crime and corruption in generally
Food security
Policy
Land
Air
Water
Energy
Minerals
Economy
Resource availability and use

Figure 18: Structuring of threats with main interdependencies

Figure 19 shows the identified threats as well as the overlaps between the suggested clusters. As an example *climate change* is a threat to land, air, water and energy and all fields are threaten by *demographic* and *disaster events*.

Summarizing the results of the first work session it is obvious, that as shown by the figure 19 below, some of the identified threats were identical to the existing list like for example *habitat loss and degradation* or *air, water and soil pollution*. Some other initial threats are sub-threats of other threats, like *invasive species* or *deforestation* are the sub-threats of *habitat degradation*. Furthermore the group identified also new threats or reformulated initial threats: *climate change*, *urbanisation* (see chapter 1.3.2), *industrialisation/ de-industrialisation* and *demographics*. *Demographics* was defined as a combination of five different developments: demographic change, movement of populations, population explosion, change in family unit size and ageing etc. as well as movements towards mega-cities.

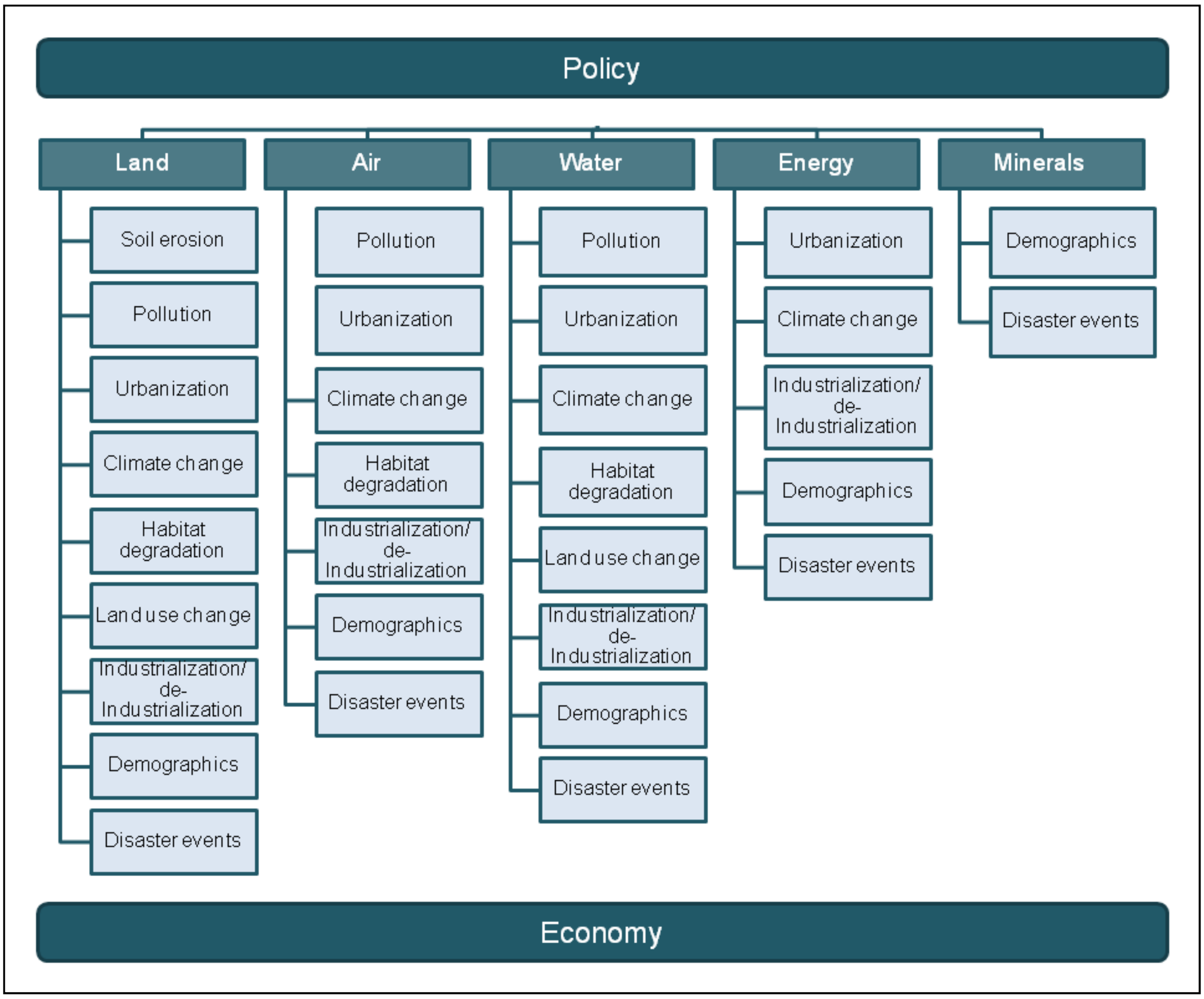


Figure 19: Mapping and clustering environmental threats

The discussion about classifying of threats was crucial for the further work in the next session. Taking these results and conclusions into account, the initial list of threats was revised and extended:

Threats which cause further threats:

- **Soil erosion** with sub-threats: deterioration or loss of ecosystem services, loss of arable land
- **Land pollution**
- **Air pollution**
- **Water pollution** with sub-threats: pharmaceutical residues from pharmaceutical discharges or residues of veterinary drugs, plastic garbage patches
- **Urbanisation** with sub-threats: loss of arable land, crime and corruption
- **Climate change** with sub-threats: greenhouse effect/ global warming, deterioration or loss of ecosystem services, biodiversity loss, deforestation
- **Habitat degradation**: deterioration or loss of ecosystem services, biodiversity loss, deforestation, introduction of invasive alien species
- **Land use change**: loss of arable land
- **Industrialisation/ de-industrialisation** with sub-threat: loss of arable land
- **Demographics**

- **Disaster events** (initial threat: "Natech" disasters - natural disasters in combination with man-made accidents)

Threats which are effects of other threats:

- Resource access triggered conflicts within and between states
- Growing western dependency on oil, gas and import of minerals and high tech metals
- Food security sub-threat: crime – food fraud and food terrorism
- Crime and corruption with sub-threat: crime – food fraud and food terrorism
- Resource availability and use (initial threat: complex nexus among resources scarcity - food, water, energy & minerals)

1.3.2 Identifying societal security needs

The second session focused on deriving societal security needs resulting from a threat which occurs in at least two different scenarios. After the presentation and short discussion of the environmental scenarios the group discussed and worked out in detail two different threats, urbanisation and disaster. It was a conscious choice, thus the first threat refers to a process and has a procedural character and the second one has an event character. In both cases the group followed the same approach:

- Definition of the selected threat based on the developed structure of threats;
- Identification of the threat effects following the key questions: In which areas might the threat be relevant? For which institutions might this threat be relevant? For which regions/ states might this threat be most relevant? What kind of influence might this threat have on these areas/ institutions/ regions? What might be potential risks?
- Deriving societal security needs based on scenarios: The starting point was the scenario “Neither awareness nor action” (yellow scenario), thus the group assumed, that in this scenario the most needs might arise. The scenario “Regulating sustainability” (orange scenario) was chosen for its diversity to the yellow one (see the overview of the scenarios in chapter 2 and the detailed descriptions in appendix).

For the second and third step the group defined what it understands under “society” and “institution” (see figure 20).

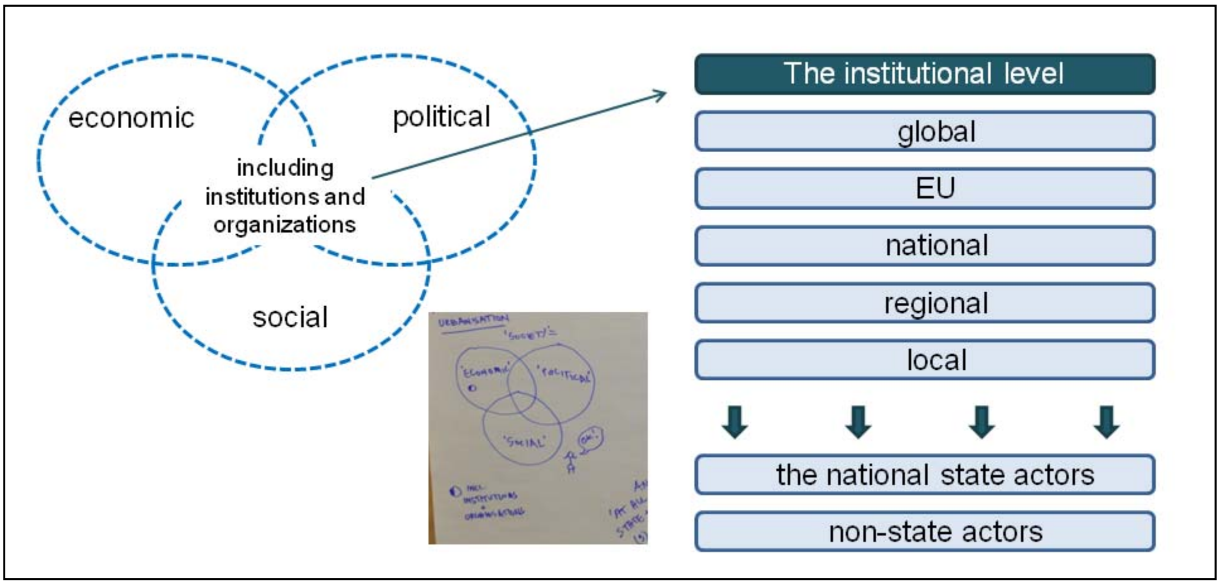


Figure 20: Definition of the society and institutional level

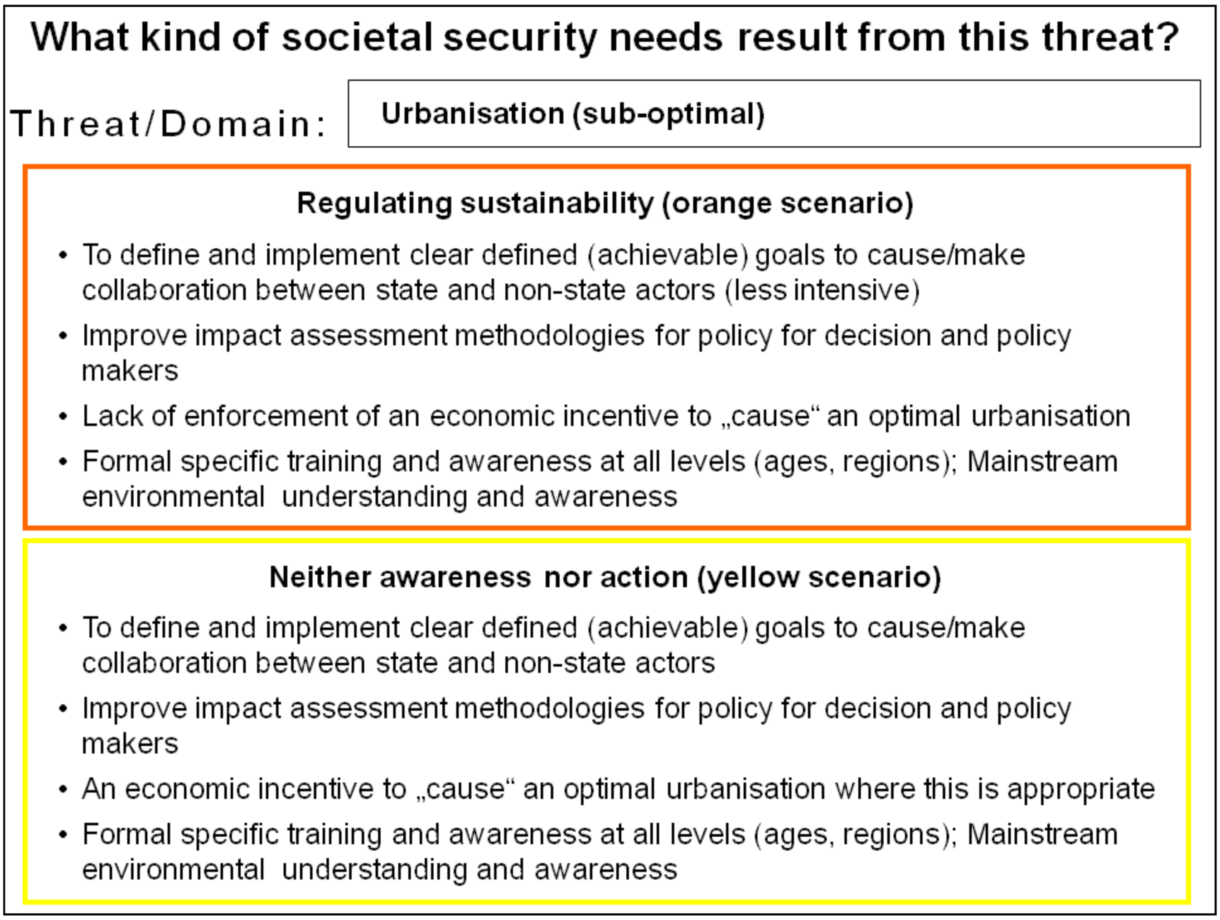
The tables 2 and 3 show the results of the first two steps for each threat. The identified societal security needs are described in the figures 21 and 22 below.

Definition	There is an optimal level of urbanisation which does not need to be a threat. A **sub-optimal urbanisation** is a threat. Urbanisation is a **process** by which the built environment is intensively and extensively developed. Historically, people have moved to cities due to demographic change, conflict, and in search of economic improvement / efficiency, lifestyle quality. But also, demographic and economic change, politics and lifestyle choice cause urbanisation, and it in turn causes demographic and economic change. **Physical effects** • Increase in intensity of land use in built environment • Building on unbuilt land in any form • ‚Sealing of the surface‘ • More people live in the same place **Societal effects** • It causes increased conflict for land resources, for services, etc. • Increased pressure on social cohesion as well as increased opportunity of density of population • Anonymity • Economic efficiency: strain on limited resources and services
Caused by	• demographic change • economic change • politics • “lifestyle” choice
Who or what is affected? In which **areas** might the threat be relevant?	Different communities are affected differently by different types of urbanisation • Social relations and cohesion • Cultural values • The “environment” (natural) • Land use (built and unbuilt land) • Use of resources
For which **institutions** might this threat be relevant? What kind of influence might this threat have on these areas/ institutions?	All level of institutions including state and non-state actors, e.g. at EU-level: • Land use policy • Environmental investment in infrastructure • Transnational relations • Land use
What might be **potential risks**?	e.g. risks for land use • Policy conflicts, e.g. environmental vs. land use • Unequal distributions of resources, e.g. tensions infrastructure vs. environment • Corruption/ crime e.g. risks for social relations and cohesion: • Societal fracture • Anonymity
For which **regions/ states** might this threat be most relevant?	• Regions at “extremities”, peripheral or very dense (non-sub-optimal) • Newer member states: • Bad challenges: corruption, environment degradation, inequalities

Table 2: Definition and effects of the threat *urbanisation (sub-urbanisation)* in overview

Due to the complexity of the *urbanisation* effects the group identified societal security needs using the example “risks for land use” and formulated general societal security needs which were transferred to environmental scenarios in the next step (see figure 21):

- Collaboration between state and non state actors;
- Connected evidence based policy making at all levels which involves how to deal with unintended consequences (before they happen);
- The definition of the “optimal” urbanisation is contextual, thus there is a need to define the „optimal“ urbanisation;
- Civil society engagement: education, awareness, authority and participation.



What kind of societal security needs result from this threat?

Threat/Domain: **Urbanisation (sub-optimal)**

Regulating sustainability (orange scenario)

- To define and implement clear defined (achievable) goals to cause/make collaboration between state and non-state actors (less intensive)
- Improve impact assessment methodologies for policy for decision and policy makers
- Lack of enforcement of an economic incentive to „cause“ an optimal urbanisation
- Formal specific training and awareness at all levels (ages, regions); Mainstream environmental understanding and awareness

Neither awareness nor action (yellow scenario)

- To define and implement clear defined (achievable) goals to cause/make collaboration between state and non-state actors
- Improve impact assessment methodologies for policy for decision and policy makers
- An economic incentive to „cause“ an optimal urbanisation where this is appropriate
- Formal specific training and awareness at all levels (ages, regions); Mainstream environmental understanding and awareness

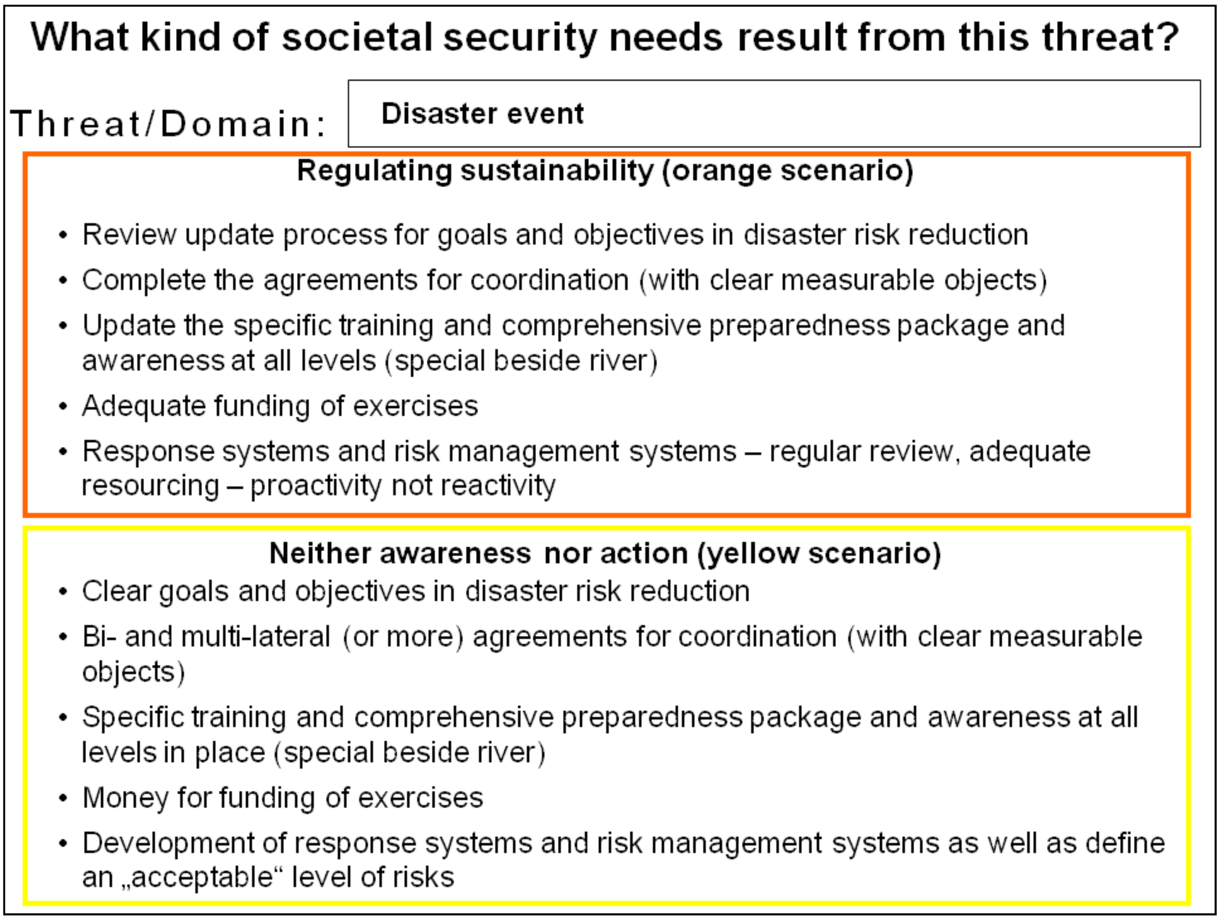
Figure 21: Scenario-based deriving of societal security needs from the threat urbanisation

Definition	Disaster is a hazard which is not appropriate managed. There are different types of disaster events: **Technical** • cyber collapse • nuclear • chemical plant fails • dam fails **Natural** • flood • volcano • earth quake • fire • pandemics **Economic** • markets fail
Caused by	**Technical** • software fails intentional and unintentional • cascading effect • crime e.g. terrorism **Natural** • natural processes • anthropogenic change **Economic** • cascading effect • crime e.g. terrorism
Who or what is affected? In which **areas** might the threat be relevant?	There are varying degrees of effects, localized or not (the scale is relevant). • Health and livelihoods of people • Social relations and cohesion • The environment • Land use (built and unbuilt land) • Access to resources (incl. economic resources)
For which **institutions** might this threat be relevant? What kind of influence might this threat have on these areas/ institutions?	All level of institutions including state and non-state actors. Whole society is affected. • Loss of life • Loss of livelihood • Loss of societal cohesion • Conflict due to the land use change • Disability/ injury • Loss of property
What might be **potential risks**?	• Damage to health • Damage to natural environment • International political implications • Initiation of further “disaster events” • Damage to image of place
For which **regions/ states** might this threat be most relevant?	see above

Table 3: Definition and effects of the threat *disaster event* in overview

The general societal security needs of the threat *disaster event* (e.g. Danube catchment) are (see the transfer to scenarios in figure 22):

- Disaster risk reduction policy;
- Collaboration state and non-state actors; international/ trans-boundary coordination;
- Awareness raising and education;
- “Real” exercise/ simulation on-site;
- Response procedures.



What kind of societal security needs result from this threat?

Threat/Domain: Disaster event

Regulating sustainability (orange scenario)

- Review update process for goals and objectives in disaster risk reduction
- Complete the agreements for coordination (with clear measurable objects)
- Update the specific training and comprehensive preparedness package and awareness at all levels (special beside river)
- Adequate funding of exercises
- Response systems and risk management systems – regular review, adequate resourcing – proactivity not reactivity

Neither awareness nor action (yellow scenario)

- Clear goals and objectives in disaster risk reduction
- Bi- and multi-lateral (or more) agreements for coordination (with clear measurable objects)
- Specific training and comprehensive preparedness package and awareness at all levels in place (special beside river)
- Money for funding of exercises
- Development of response systems and risk management systems as well as define an „acceptable“ level of risks

Figure 22: Scenario-based deriving of societal security needs from the threat disaster event

2 Identifying societal security needs – final results

In addition to the discussions of the scenario validation workshop, further activities to identify social security needs were a part of WP4: Firstly, the interviews with stakeholders in task 4.1 (the relevant results are presented in D.4.4) and, secondly, the analysis of security related future studies. This research-based analysis of needs contained i.e. defining terms, structuring the existing classifications of needs as well as the transfer of these results to the field of security, in particular to cyber infrastructure, nuclear and environment. There are important methodological insights from this analysis which will be transferred to WP3 (see D.4.2).

For this purpose we analysed systematically a wide range of secondary sources, like literature related to the needs in general (for defining terms and structuring the existing classifications of needs) as well as various future studies and research works with focus on future developments and related to the fields of security, in particular cyber infrastructure, nuclear and environment (transfer of the theoretical findings). In addition the findings of task 2.2 (see D.2.2) were used, which provide an in-depth analysis of the key trends emerging from completed and ongoing foresight and other relevant security projects, undertaken both, in Europe and beyond.

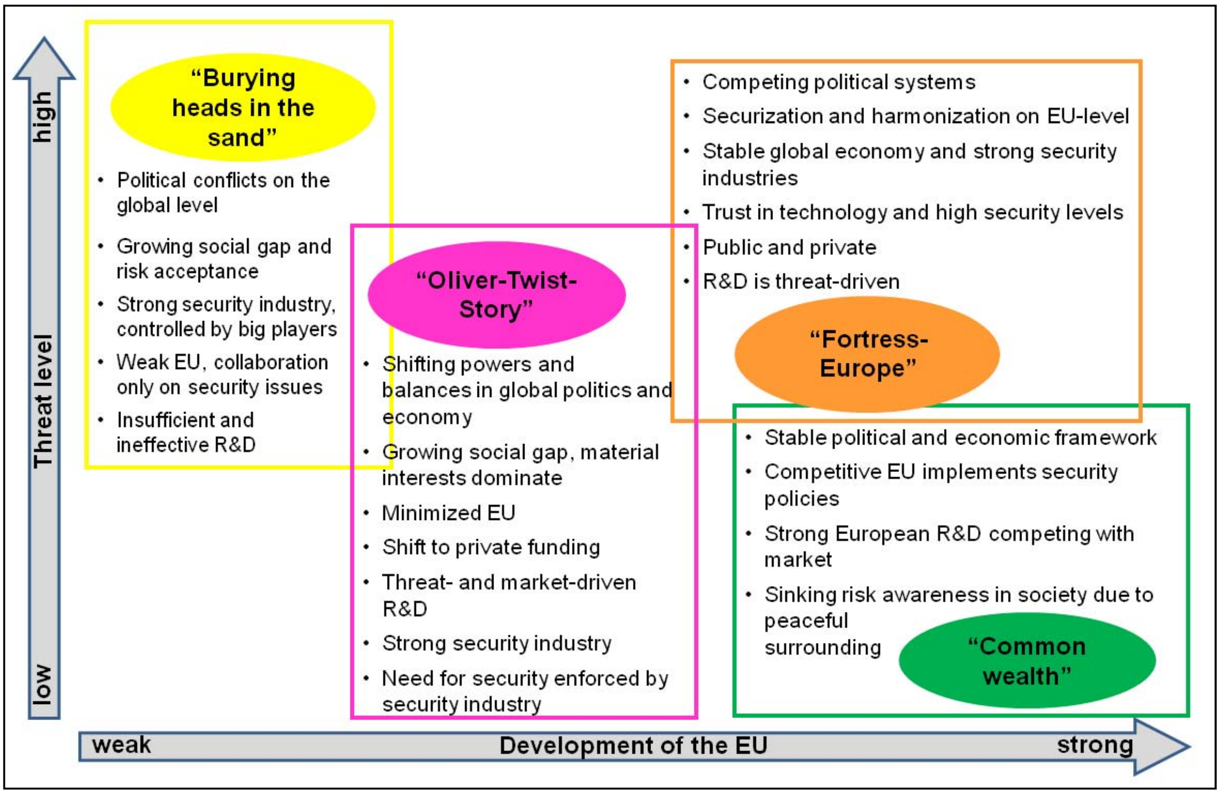
These documents represented different organisations, e.g. think tanks, other NGOs, research institutions and academia. Although we have particularly focused on European-funded research projects, we have also reviewed projects outside the EU. The following questions have been driving our investigation:

- What are the most important needs in the field of security today and in the future?
- What are the most important needs in the domains cyber infrastructure, nuclear and environment?
- From which threats could these needs result?
- Who is affected by a specific threat? What regions are affected?

The findings of the **interviews with stakeholders in task 4.1**, **analysis of security related future studies** as well as the **findings of WP2** combined with the **findings from the scenario validation workshop** are summarized in chapters 2.1 to 2.3 (see tables 4 to 6). Thus there are overlaps between the need identified for different scenarios and within different domains, a consolidated list of societal security needs was developed (see table 7, chapter 2.4).

The societal security needs which may be derived from the identified threats were to the scenarios in which they may occur. The impact level describes the expected societal impact of a threat. Legend: red = high impact; yellow = medium impact, green = less impact. Please note that the colours do **not indicate a level of probability** that one of these threats will occur. It only refers to the expected level of societal impact in case it occurs.

As described in the previous chapter, scenarios were built at two levels, context scenarios (global security scenarios) and threat scenarios (scenarios of cyber infrastructure, nuclear and environment). The deriving of societal security needs based on four context based threats scenarios. Figure 23 shows an overview of the characteristics of the context scenarios which built the framework conditions for developing the threats scenarios. The overviews of the threat scenarios are presented in chapters 2.1 to 2.3 (see figures 24 to 26). The appendix contains the detailed descriptions of all scenarios (see also D.4.4).



high
Threat level
low
weak
Development of the EU
strong
"Burying heads in the sand"
• Political conflicts on the global level
• Growing social gap and risk acceptance
• Strong security industry, controlled by big players
• Weak EU, collaboration only on security issues
• Insufficient and ineffective R&D
"Oliver-Twist-Story"
• Shifting powers and balances in global politics and economy
• Growing social gap, material interests dominate
• Minimized EU
• Shift to private funding
• Threat- and market-driven R&D
• Strong security industry
• Need for security enforced by security industry
• Competing political systems
• Securization and harmonization on EU-level
• Stable global economy and strong security industries
• Trust in technology and high security levels
• Public and private
• R&D is threat-driven
"Fortress-Europe"
• Stable political and economic framework
• Competitive EU implements security policies
• Strong European R&D competing with market
• Sinking risk awareness in society due to peaceful surrounding
"Common wealth"

Figure 23: Characteristics of the context scenarios in overview

"Common wealth" (green scenario)

In this scenario big efforts are made towards more resilience and there is an absence of great power conflicts on the global level. The EU is competitive and on the global level there is also a long-term economic stability. There is a strong industrial capability and knowledge base in the security field in Europe. A main focus of the EU is to achieve a worldwide leading position in R&D as well as in security industry. Due to the declining need for security, the risk awareness of the society is sinking. Technology acceptance also differs, depending on its characteristics like suitability for daily use etc. Traditional and social values still remain important in the European countries. Topics like active ageing, life-long education, demographic change and new living models play a significant role.

"Fortress Europe" (orange scenario)

The global situation is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive. In the European countries the 'western' value system remains important, but there is a strong focus on securitisation of life, pushed forward by the extensive Security Policy of the EU and a fragmented, yet strong security economy and industry. Despite the high technology penetration of everyday life, people trust in technological solutions. For higher security level, citizens even reduce the claims to their fundamental rights and for high security standards, public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

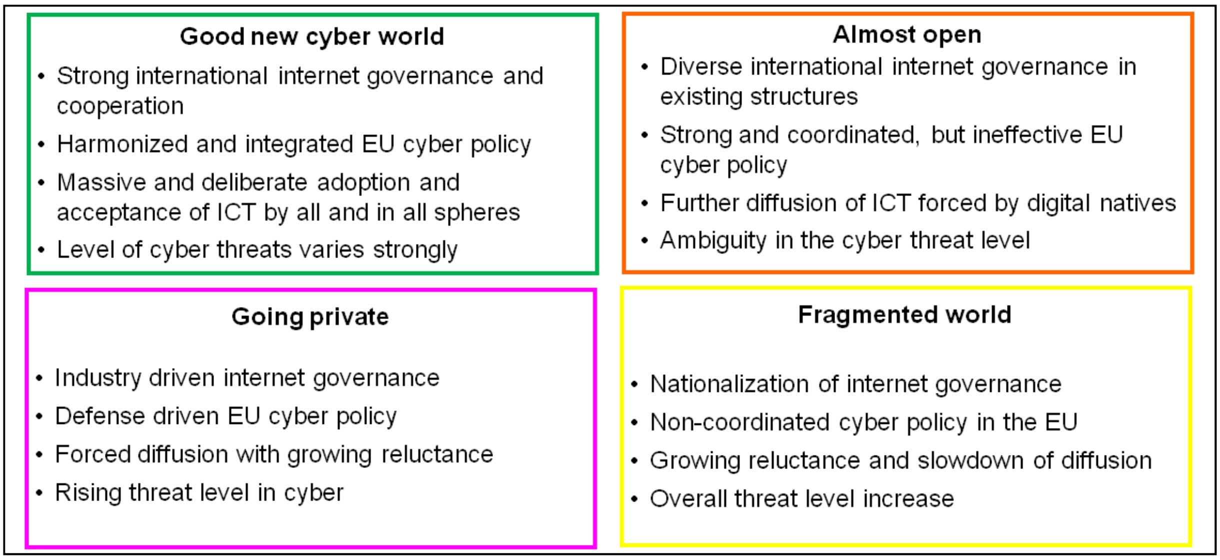
"Oliver-Twist-Story" (pink scenario)

This scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. There is a strong security industry by a fragmented market. The European security industry is very strong and produces customized security solutions for society. User-friendliness is rather oriented on market interests than on the best solution. There is a high technology penetration of everyday life but also trust in technological solutions. For higher security levels, people tend to reduce their rights. In society technologies are seen as a solution for security challenges. Resulting from the economical situation, the society attaches more importance to material interests than to traditional and social values. The social gap grows further and there is a strict differentiation between social classes.

“Burying heads in the sand” (yellow scenario)

The worldwide situation is marked by many conflicts. The global political and economic situation is instable and the EU also loses its power. Global powers and balances shift to few regions and there are conflicts over markets. The long-term financial crisis is not overcome. The market is determined by multinational companies and big players which concentrate on markets with few risks. Still US companies dominate the security market. The social gap grows further and there is a strict differentiation between social classes. As an effect of these developments, extreme groups become stronger and are difficult to control. The society is aware that not all risks may be covered by security solutions. Technology acceptance is decreasing in general, more effective research is required.

2.1 Cyber infrastructure



Good new cyber world

- Strong international internet governance and cooperation
- Harmonized and integrated EU cyber policy
- Massive and deliberate adoption and acceptance of ICT by all and in all spheres
- Level of cyber threats varies strongly

Almost open

- Diverse international internet governance in existing structures
- Strong and coordinated, but ineffective EU cyber policy
- Further diffusion of ICT forced by digital natives
- Ambiguity in the cyber threat level

Going private

- Industry driven internet governance
- Defense driven EU cyber policy
- Forced diffusion with growing reluctance
- Rising threat level in cyber

Fragmented world

- Nationalization of internet governance
- Non-coordinated cyber policy in the EU
- Growing reluctance and slowdown of diffusion
- Overall threat level increase

Figure 24: Characteristics of the cyber infrastructure scenarios in overview

Cyber infrastructure threats	Societal security needs	Good new cyber world (green scenario)	Almost open (orange scenario)	Going private (pink scenario)	Fragmented world (yellow scenario)
"Second world" problem	a. Control of supplier b. Awareness raising c. Prevention	a, b	a, b	a, b, c	a, b, c
Accidental network breakdown	a. Prevention b. Crisis Management c. Control d. Technological solutions Certification of providers	b, e	a, b, c	a, b, c, d	a, b, c, d
Backslash	a. Trust building b. Training	🟩	🟩	a, b	a
Civil engagement in digital worlds	a. Awareness b. Training and education for all users	a, b	a, b	a, b	a, b
Commercial cyber espionage	a. Awareness raising b. Educational measures c. Technical solutions d. Enforcement prosecution	a, b, c	a, b, c	a, b, c, d	a, b, c, d
Commercial disinformation	a. Transparency of data b. Clear traceability of origin c. Awareness raising	a, b, c	a, b, c	a, b, c	a, b, c
Commercial reputation manipulation	a. Transparency of data b. Clear traceability of origin c. Awareness raising d. Educational measures	🟩	a, b, c	a, b, c	a, b, c, d
Criminal cyber extortion	a. Awareness raising b. Prevention technologies c. Proactive measures d. Prosecution	a, b, c, d	a, b, c, d	a, b, c, d	a, b, c, d

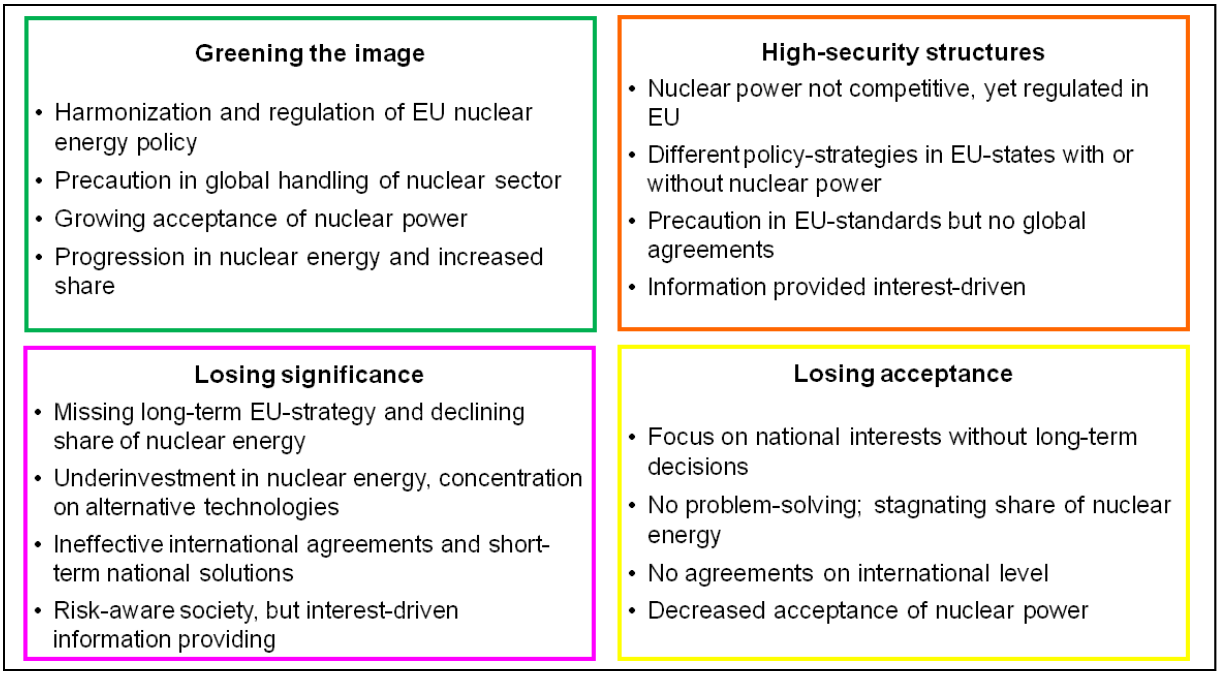
Cyber bullying/ mobbing	a. Traceability of identity. b. Awareness raising c. Training d. Prosecution	a, b, c	a, b, c	a, b, c, d (enforced)	a, b, c, d
Cyber warfare	a. Regulation/ban b. Protection c. Management d. Countermeasures	a, b, c	a, b, c	a, b, c, d	a, b, c, d
Data loss, leak and trading	a. Training b. Awareness c. Technical measures d. Control	a, b	a, b, c, d	a, b, d	a, b, c, d
Data trails	a. Training b. Awareness c. Regulation data protection	🟩	a, b, c	a, b, c	a, b, c
Digital currency laundry	a. Prevention b. Certification c. Awareness d. Prosecution e. Control of suppliers	🟩	a, b, c	a, b, c, d, e	a, b, c
Digital pocket picking	a. Technical protection b. Awareness c. Training	🟩	a, b	a, b, c	a, b, c
Digital vigilantism	a. Prevention measures b. Awareness c. Training d. Control	a, b, c, d	a, b, c, d	a, b, c, d	a, b, c, d
Easy availability of tools	a. Control b. International cooperation c. Prosecution	🟩	a, b, c	a, b, c	a, b
Global footprint	a. Awareness b. Recycling management alternatives	🟩	🟩	a, b	a, b
Governmental cyber espionage	a. Detection and prevention b. Certification c. Technical measures d. Counter measures	a, b, c	a, b, c	a, c, d	a, b, c, d
Governmental sabotage	a. Prevention b. Protection c. Preparedness	a, b, c	a, b, c, d	a, b, c, e	a, b, c, e

	d. Technical solutions e. Counter measures	🟨	🟨	🟨	🟨
Hacktivism and disproportion	a. Protection b. Security speech c. Balance of reaction d. Anonymity	🟩	🟨 b, c, d	🟥 a, b, c, d	🟥 a, b, c, d
Identity challenges	a. Clear identity rules b. Fraud/burglary protection c. Awareness d. Training	🟨 a, b, c, d	🟨 a, b, c, d	🟥 a, b, c, d	🟥 a, b, c, d
Insider attacks	a. Prevention b. Certification c. Proactive technologies d. Increased control	🟨 a, b, c	🟨 a, b, c	🟥 a, b, c, d	🟥 a, b, c, d
Lack of (long term) data management	a. Protection measures b. Control c. Certification d. Awareness	🟩	🟨 a, b, c, d	🟨 a, b, c, d	🟨 a, b, c, d
Limits of growth	a. Technological measures	🟩	🟨 a	🟨 a	🟨 a
Monopolisation of digital business	a. Regulation of power b. Anti-trust regulation c. Better protection of customer rights d. Awareness raising e. Support for alternatives	🟩	🟨 a, b	🟨 b, c, d, e	🟥 a, b, c, d
Opinion bias	a. Transparency of lobbying b. Better participation technologies c. Improved measures	🟩	🟩	🟨 a, b, c	🟨 a, b, c
Political disinformation	a. Transparency of data b. Clear traceability of origin c. Awareness raising	🟨 a, b, c	🟨 a, b, c	🟨 a, b, c	🟨 a, b, c
Privacy desensitisation	a. Right to deletion b. Right to be informed c. Better protection through clear regulation	🟨 a, b, c	🟨 a, b, c	🟥 a, b, c	🟨 a, b, c
Software as an institution	a. Clear rules for usage, b. Transparency of processes c. Control of use	🟨 a, b, c	🟨 a, b, c	🟥 a, b, c	🟨 a, b, c

System complexity	a. Better information b. Prevention c. Proactive management d. Crisis management e. Awareness raising	🟨 a, b, c	🟨 a, b, c	🟥 a, b, c, d, e	🟥 a, b, c, d, e
Targeted network breakdown	a. Prevention measures b. Proactive management c. Complexity control d. Awareness raising	🟩	🟨 a, b, c	🟥 a, b, c, d	🟥 a, b, c, d
Terroristic sabotage	a. Techniques for prevention b. Crisis management c. Security improvements	🟥 a, b, c	🟥 a, b, c	🟥 a, b, c	🟥 a, b, c
Thievery/ burglary	a. Prevention technologies b. Detection c. Awareness d. Educational measures	🟨 a, b, c	🟨 a, b, c	🟨 a, b, c, d	🟨 a, b, c, d
Unclear data ownership and governance	a. IPR regulation b. Data protection and privacy c. Awareness d. Regulation	🟩	🟨 a, b	🟨 a, b, c, d	🟨 a, b, c
Unexpected data fusion	a. Better customer data protection b. IPR for data c. Possibility to delete data	🟩	🟨 a, b, c	🟥 a, b, c	🟨 a, b, c
Virtual crime communities	a. Traceability of identity b. Awareness c. Support of civic engagement d. Prevention by technical means	🟥 a, b, c	🟥 a, b, c, d	🟥 a, b, c, d	🟥 a, b, c, d

Table 4: Deriving of societal security needs based on threat scenarios of cyber infrastructure

2.2 Nuclear



Greening the image

- Harmonization and regulation of EU nuclear energy policy
- Precaution in global handling of nuclear sector
- Growing acceptance of nuclear power
- Progression in nuclear energy and increased share

High-security structures

- Nuclear power not competitive, yet regulated in EU
- Different policy-strategies in EU-states with or without nuclear power
- Precaution in EU-standards but no global agreements
- Information provided interest-driven

Losing significance

- Missing long-term EU-strategy and declining share of nuclear energy
- Underinvestment in nuclear energy, concentration on alternative technologies
- Ineffective international agreements and short-term national solutions
- Risk-aware society, but interest-driven information providing

Losing acceptance

- Focus on national interests without long-term decisions
- No problem-solving; stagnating share of nuclear energy
- No agreements on international level
- Decreased acceptance of nuclear power

Figure 25: Characteristics of the nuclear scenarios in overview

Nuclear threats	Societal security needs	Greening the image (green scenario)	High-security structures (orange scenario)	Loosing significance (pink scenario)	Loosing acceptance (yellow scenario)
Accidents while nuclear decommissioning	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public participation / engagement / information after CBRN incident e. Public health protection (radiological / psychological) f. Preparing measures for mitigation g. Maintaining a skilled, knowledgeable workforce h. Fast recovery	b, d, e, f, h	c, d, e, f, h	a, b, c, d, e, f, g, h	a, c, d, e, f, g, h
Accidents during nuclear material transport	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public participation / engagement / information after CBRN incident e. Public health protection (radiological / psychological) f. Higher need to prepare measures for mitigation g. Maintaining a skilled, knowledgeable workforce h. Fast recovery	b, d, e, f, h	c, d, e, f, h	a, b, c, d, e, f, g, h	a, c, d, e, f, g, h
Radiological threats from sources outside the nuclear industry	a. Protection of peoples' health b. Improved recycling management	a, b	a, b	a, b	a, b
Higher risk of nuclear accidents during transport in countries with new nuclear programs	a. Safety culture b. Regulation (safety and security) c. Qualified workers	b, c	a, c	a, b, c	a, b, c

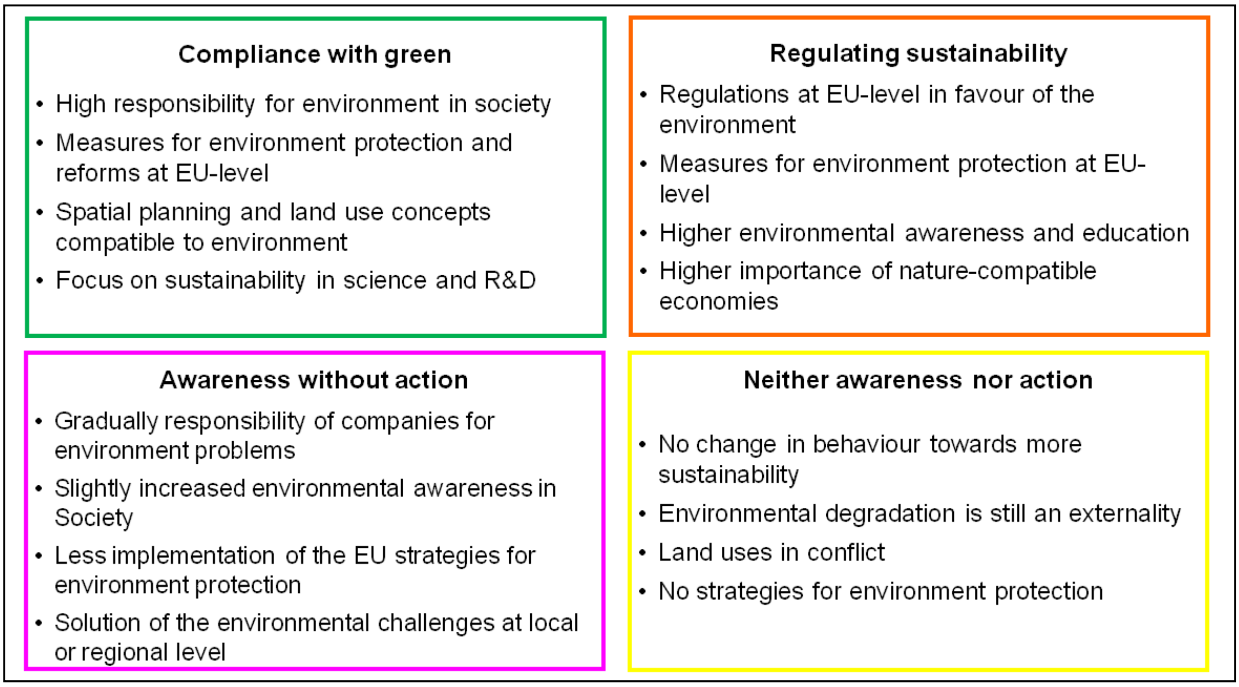
Accidents by nuclear shutdown	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public participation / engagement / information after CBRN incident e. Public health protection (radiological / psychological) f. Preparing measures for mitigation g. Maintaining a skilled, knowledgeable workforce h. Power supply security i. Fast recovery	b, d, e, h, i	c, d, e, f, h, i	a, b, c, d, e, f, g, h, i	a, c, d, e, f, g, h, i
Nuclear power plant accident during operation of plant	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public health protection (radiological / psychological) e. Preparing measures for mitigation f. Maintaining a skilled, knowledgeable workforce g. Fast recovery	b, d, e, g	b, c, d, e, g	a, b, c, d, e , f, g	a, b, c, d, e, f, g
Low levels of trust in institutions may lead to fear in society and risk of accidents	a. Reducing fear in some parts of society b. Reducing risks of accidents c. Effective regulations d. More public attention and control e. Trust and comprehension of the citizens in government (instead in experts with high media attention)	a, b, e	a, b, d	a, b, c, d, e	a, b, c, d, e
Higher risk of nuclear accidents in countries with new nuclear program during operation of a nuclear power plant	a. Safety culture b. Regulation (safety and security) c. Maintaining a skilled, knowledgeable workforce d. More public attention and control	a, b, d	b, c, d	a, b, c, d	a, b, c, d
Accidents in front end nuclear fuel cycle causing health threats (like uranium mining)	a. Strong safety culture b. Good crisis management c. Public participation / engagement / information after CBRN incident d. Public health protection (radiological / psychological) e. Preparing measures for mitigation f. Maintaining a skilled, knowledgeable workforce	a, c, d, e	b, c, d, e	a, b, c, d, e , f	a, b, c, d, e, f

Accidents in nuclear waste storage	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public participation / engagement / information after incident e. Public health protection (radiological / psychological) f. Preparing measures for mitigation g. Maintaining a skilled, knowledgeable workforce h. Fast recovery	🟨 b, d, e, f, h	🟨 c, d, e, f, h	🟥 a, b, c, d, e, f, g, h	🟥 a, c, d, e, f, g, h
Safety threats caused by accidents due to exceeded regulatory maturity	a. Strong safety culture b. Public reassurance / confidence → need to mitigate psychological impacts c. Good crisis management d. Public participation / engagement / information after incident e. Public health protection (radiological / psychological) f. Preparing measures for mitigation g. Maintaining a skilled, knowledgeable workforce h. Fast recovery	🟥 b, d, e, f, h	🟥 c, d, e, f, h	🟥 a, b, c, d, e, f, g, h	🟥 a, c, d, e, f, g, h
Loss of nuclear and radiological material, e.g. during transport, causing safety and security threats	a. R&D on waste recycling b. Better international regulation & control system c. Maintaining a skilled, knowledgeable workforce d. Detection and localisation of nuclear substances crossing unregulated land borders	🟨 a, b, c, d	🟨 a, b, c, d	🟥 a, b, c, d	🟥 a, b, c, d
Nuclear proliferation causing security threats	a. Multilateral agreements, confidence building in place b. Less prescriptive regulation, strong industry contribution c. Control of international enriched nuclear fuel supply d. Increased involvement needed from political and international actors (due to decline in industry) e. More prescriptive regulatory regime → risk assessment by political actors	🟥 a, b, c	🟥 a, b, c	🟨 a, c, d, e	🟨 A, c, d, e
Security threats due to nuclear espionage for proliferation	a. Multilateral agreements, confidence building in place b. Less prescriptive regulation, strong industry contribution c. Control of international enriched nuclear fuel supply d. Increased involvement needed from political and international actors (due to decline in industry) e. More prescriptive regulatory regime → risk assessment by political actors	🟨 a, b, c	🟨 a, b, c	🟩 a, c, d, e	🟨 A, c, d, e
Security threats due to nuclear tests for proliferation	a. Multilateral agreements, confidence building in place b. Less prescriptive regulation, strong industry contribution c. Control of international enriched nuclear fuel supply d. Increased involvement needed from political and international actors (due to decline in industry) e. More prescriptive regulatory regime → risk assessment by political actors	🟥 a, b, c	🟥 a, b, c	🟨 a, c, d, e	🟨 A, c, d, e

Theft of radiological materials/ nuclear technology during nuclear material transport	a. Multi-lateral agreements for inspections and inventory b. Mutual assurance of international regulation (mitigation) c. Protection of facilities d. High security measurements during transportation e. Prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer etc.	🟨 a, c, d, e	🟨 a, b, c, d, e	🟨 b, c, d, e	🟨 b, c, d, e
Theft of radiological materials/ nuclear technology by nuclear espionage	a. Multi-lateral agreements for inspections and inventory b. Mutual assurance of international regulation (mitigation) c. Protection of facilities d. Prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer etc.	🟨 a, c, d	🟨 b, c, d	🟥 b, c, d	🟥 b, c, d
Theft of radiological materials/ nuclear technology due to international organized crime and illegal trafficking	a. Multi-lateral agreements for inspections and inventory b. Mutual assurance of international regulation (mitigation) c. Protection of facilities d. Prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer etc.	🟨 a, b, c, d	🟨 a, b, c, d	🟥 a, b, c, d	🟥 a, b, c, d
Terrorist attacks (cyber; physical), may occur by nuclear espionage	a. Better protection of facilities b. Addressing root causes of terrorism c. Intelligence on terrorist groups / prevention d. Response preparation e. Public communication about risks f. Global surveillance of WMD and CBRN weapons	🟥 b, c, e	🟥 a, b, c, d, e	🟥 a, b, c, d, e	🟥 a, b, c, d, e

Table 5: Deriving of societal security needs based on threat scenarios of nuclear

2.3 Environment



Compliance with green

- High responsibility for environment in society
- Measures for environment protection and reforms at EU-level
- Spatial planning and land use concepts compatible to environment
- Focus on sustainability in science and R&D

Regulating sustainability

- Regulations at EU-level in favour of the environment
- Measures for environment protection at EU-level
- Higher environmental awareness and education
- Higher importance of nature-compatible economies

Awareness without action

- Gradually responsibility of companies for environment problems
- Slightly increased environmental awareness in Society
- Less implementation of the EU strategies for environment protection
- Solution of the environmental challenges at local or regional level

Neither awareness nor action

- No change in behaviour towards more sustainability
- Environmental degradation is still an externality
- Land uses in conflict
- No strategies for environment protection

Figure 26: Characteristics of the environment scenarios in overview

Environment threats	Societal security needs	Compliance with green (green scenario)	Regulating sustainability (orange scenario)	Awareness without action (pink scenario)	Neither awareness nor action (yellow scenario)
Soil erosion (deterioration or loss of ecosystem services, loss of arable land)	a. Protection of important ecosystem services b. Support the capacity of ecosystems to tolerate disturbance without collapsing c. Risks assessment modelling	a, b	a, b	a, b, c	a, b, c
Land pollution	a. Being able to have good health, including reproductive health b. Unpolluted food; examination of food c. Risks assessment modelling and impact reduction d. Tools for neutralisation of pollution	b, d	b, d	a, b, c, d	a, b, c, d
Air pollution	a. Efficient common international mitigation policy and agreements b. Identification with same goals, same actions c. Not reducing of the human life quality d. Being able to have good health, including reproductive health e. Unpolluted and fresh air; methodology to identify new relevant contaminates in air f. Tools for neutralisation of pollution	a, b, e, f	a, b, e, f	a, b, c, d, e, f	a, b, c, d, e, f
Water pollution due to pharmaceutical residues from pharmaceutical discharges or residues of veterinary drugs or due to plastic garbage patches	a. Efficient common international mitigation policy and agreements b. Identification with same goals, same actions c. Being able to have good health, including reproductive health d. Unpolluted and fresh water; methodology to identify new relevant contaminates in water e. Tools for neutralisation of pollution	a, b, d, e	a, b, d, e	a, b, c, d, e	a, b, c, d, e
Climate change (greenhouse effect/ global warming)	a. Efficient common international mitigation policy and agreements b. Identification with same goals, same actions c. Not reducing of the human life quality d. Stable climate e. Spread the knowledge about climate change and its consequences in society f. Support the adaption to climate change	a, b, d, f	a, b, d, f	a, b, c, d, e, f	a, b, c, d, e, f

Habitat degradation (deterioration or loss of ecosystem services, biodiversity loss, deforestation, introduction of invasive alien species)	a. Efficient international environmental policy and agreements b. Continuously improvement of regulations taking into account new challenges, technical progress and international regulations c. Identification of best practices for environment protection d. Protection of important ecosystem services e. Support the capacity of ecosystems to tolerate disturbance without collapsing f. Job security g. Biological variety	🟩 a, b, d, g	🟨 a, b, c, d, g	🟨 a, b, c, d, e, f, g	🟥 a, b, c, d, e, f, g
Sub-optimal urbanisation (loss of arable land, crime and corruption)	a. Clear definition and implementation of achievable goals to support collaboration between state and non-state actors b. Improve impact assessment methodologies for decision and policy makers c. An optimal urbanisation where this is appropriate d. Qualification and awareness in society at all levels (ages, regions); Mainstream environmental understanding and awareness e. Disaster risks management in urban areas f. Fighting against the corruption	🟩 a, c, d	🟨 a, b, c (enforcement), d	🟥 a, b, c, d	🟥 a, b, c, d
Land use change (loss of arable land)	a. Clear definition and implementation of achievable goals to support collaboration between state and non-state actors b. Improve impact assessment methodologies for decision and policy makers	🟩 a	🟩 a, b	🟨 a, b	🟥 a, b
Industrialisation/ de-industrialisation with sub-threat (loss of arable land)	a. Preserve agrarian society and the perception of nature b. Job security	🟩 a, b	🟨 a, b	🟥 a, b	🟥 a, b
Demographics	a. International agreements referring to migration b. Strategic impact planning; simulation; modeling c. Stable population d. Reproduction e. Preservation of family	🟨 c, d	🟨 a, c, d	🟥 a, b, c, d, e	🟥 a, b, c, d, e
Disaster events (also "Natech" disasters - natural disasters in combination with man-made accidents)	a. Clear goals and objectives in disaster risk reduction b. Bi- and multi-lateral agreements for coordination (with clear measurable objects) c. Comprehensive preparedness package and awareness at all levels d. Adequate funding of exercises e. Development of response systems and risk management systems f. Definition of an „acceptable“ level of risks i. Information during and after incidents j. Fast recovery k. Being able to stay alive/ have good health	🟩 a (update), f, i, j	🟨 a (update), b, c (update), d, e (regular review, pro-activity), f, i	🟨 a (update), b, c (update), d, e (regular review, pro-activity), f, i	🟥 a, b, c, d, e, f, i
Resource access triggered conflicts within and between states	a. Protection of the economic relationships between EU and other regions b. Need to maintain the access to resources, supporting economic growth c. Fighting against the corruption	🟩 a, b	🟨 a, b	🟥 a, b, c	🟥 a, b, c

Growing western dependency on oil, gas and import of minerals and high tech metals	a. Protection of the economic relationships between EU and other regions b. Need to maintain the access to resources, supporting economic growth c. Independence, autonomy d. Increasing the ability of societies to manage socio-economic-stress	a, b, c, d	a, b, c, d	a, b, c, d	a, b, c, d
Food security (crime – food fraud and food terrorism)	a. International agreements referring to resource distribution b. Prevention against social polarisation, radicalisation development and segregation c. Need to maintain the access to resources, supporting economic growth d. Being able to have good health e. Being adequately nourished; Variety of nutrition f. Self-prevention/ personal responsibility g. Fighting against the corruption	a, c, e, f	a, b, d, e, f	a, b, c, d, e, f, g	a, b, c, d, e, f, g
Resource availability and use (complex nexus among resources scarcity - food, water, energy & minerals)	a. International agreements referring to resource distribution b. Prevention against social polarisation, radicalisation development and segregation c. Need to maintain the access to resources, supporting economic growth d. Increasing the ability of societies to manage socio-economic-stress e. Not reducing of the human life quality	a, c, d, e	a, c, d, e	a, b, c, d, e	a, b, c, d, e

Table 6: Deriving of societal security needs based on threat scenarios of environment

2.4 Consolidated list of societal security needs

The tables above show the societal security needs in direct connection to the threats and scenarios for each domain. Due to the fact that different threats could have similar or the same impact, like different types of accidents or attacks, similar or the same needs result from these threats. To demonstrate the variety of the identified needs a consolidated list of needs was developed (see table 7 below, it should be noted that the needs presented in this list are vaguer than in the tables above, because there were separated from threats and scenarios).

There are overlaps between societal security needs across the domains. A few main groups are visible:

- Protection (e.g. of goods, immaterial goods, health, people),
- Regulation (e.g. implementation, improvement),
- Education, training (e.g. qualified workforce, educated society),
- Information and transparency (e.g. about risks, measures, incidents)
- International cooperation (e.g. regulation, agreements, enforcement),
- Trust, reducing fear, safety culture and responsibility (e.g. trust in government, own responsibility)
- Risk management (e.g. impact planning; simulation; modelling).

Cyber infrastructure	• Anonymity • Anti-trust regulation • Awareness raising • Balance of reaction • Certification/ Certification of providers • Clear identity rules • Clear rules for usage • Control of supplier/ Complexity control/ Control of use • Counter measures • Crisis management • Data protection and privacy/ Customer data protection • Detection • Educational measures • Improved measures • Increased control • Information • International cooperation • IPR for data • IPR regulation • Management • Participation technologies • Possibility to delete data • Prevention measures/ Prevention technologies/ Prevention by technical means • Proactive management/ Proactive measures/ Proactive technologies • Prosecution/ Enforcement prosecution • Protection/ Fraud/burglary protection/ Protection measures/ protection of customer rights/ Protection through clear regulation • Recycling management alternatives • Regulation/ Regulation data protection/ Regulation of power/ Regulation/ban • Right to be informed • Right to deletion • Security improvements • Security speech • Support for alternatives • Support of civic engagement • Technical measures/ Technical protection/ Technical solutions/ Techniques for prevention • Technological measures/ Technological solutions • Traceability of identity/ Clear traceability of origin • Training/ Training and education for all users • Transparency of data/ Transparency of lobbying/ Transparency of processes • Trust building

Nuclear	• Addressing root causes of terrorism • Better international regulation & control system • Better protection of facilities • Control of international enriched nuclear fuel supply • Detection and localisation of nuclear substances crossing unregulated land borders • Effective regulations • Fast recovery • Global surveillance of WMD and CBRN weapons • High security measurements during transportation • Higher need to prepare measures for mitigation • Improved recycling management/ R&D on waste recycling • Increased involvement needed from political and international actors (due to decline in industry) • Intelligence on terrorist groups / prevention • Less prescriptive regulation, strong industry contribution • Maintaining a skilled, knowledgeable workforce • Maintaining a skilled, knowledgeable workforce • More prescriptive regulatory regime: risk assessment by political actors • More public attention and control • Multi-lateral agreements for inspections and inventory • Multilateral agreements, confidence building in place • Mutual assurance of international regulation (mitigation) • Power supply security • Preparing measures for mitigation • Prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer et • Protection of facilities • Protection of peoples' health • Public communication about risks • Public health protection (radiological / psychological) • Public participation / engagement / information after incident/ information after CBRN incident • Public reassurance / confidence: need to mitigate psychological impacts • Qualified workers • Reducing fear in some parts of society • Reducing risks of accidents • Regulation (safety and security) • Response preparation • Safety culture/ Strong safety culture • Trust and comprehension of the citizens in government (instead in experts with high media attention)

Environment	• Adequate funding of exercises • An optimal urbanisation where this is appropriate • Being able to have good health, including reproductive health/ Being able to stay alive/ have good health • Being adequately nourished; Variety of nutrition • Bi- and multi-lateral agreements for coordination (with clear measurable objects) • Biological variety • Clear definition and implementation of achievable goals to support collaboration between state and non-state actors • Clear goals and objectives in disaster risk reduction • Comprehensive preparedness package and awareness at all levels • Continuously improvement of regulations taking into account new challenges, technical progress and international regulations • Definition of an „acceptable“ level of risks • Development of response systems and risk management systems • Disaster risks management in urban areas • Efficient common international mitigation policy and agreements • Efficient international environmental policy and agreements • Fast recovery • Fighting against the corruption • Identification of best practices for environment protection • Identification with same goals, same actions • Improve impact assessment methodologies for decision and policy makers • Increasing the ability of societies to manage socio-economic-stress • Independence, autonomy • Information during and after incidents • International agreements referring to migration/ International agreements referring to resource distribution • Job security • Need to maintain the access to resources, supporting economic growth • Not reducing of the human life quality • Preservation of family • Prevention against social polarisation, radicalisation development and segregation • Protection of important ecosystem services • Protection of the economic relationships between EU and other regions • Qualification and awareness in society at all levels (ages, regions); Mainstream environmental understanding and awareness/ Spread the knowledge about climate change and its consequences in society/ Preserve agrarian society and the perception of nature • Reproduction • Risks assessment modeling and impact reduction/ Strategic impact planning; simulation; modeling • Stable climate/ Support the adaption to climate change • Stable population • Support the capacity of ecosystems to tolerate disturbance without collapsing • Tools for neutralisation of pollution/ Unpolluted and fresh air/ Unpolluted and fresh water; methodology to identify new relevant contaminates/ Unpolluted food; examination of food

Table 7: Consolidated list of societal security needs for each domain

3 Summary and outlook of further research

The scenario validation workshop delivered input to the final task (4.5) within WP4. In order to validate the outcome of the previous scenario development process, this workshop firstly contributed to the scenario discussion as well as the discussion, further identification and the selection of threats for cyber infrastructure, nuclear and environment. Secondly, it provided additional crucial and solid groundwork for identifying societal security needs which describe what happens when a threat occurs in different scenarios. There were comprehensive discussions about threats, in particular regarding to their structure and content or relevance. Many ideas of societal security needs for selected threats were generated during the discussions. It was not possible to derive the needs from all identified threats in all domains due to the limited time; however it was not the aim of the workshop. These identified needs were captured by note takers and were taken up in the further process.

In addition to the discussions of the scenario validation workshop, further activities to identify social security needs were a part of WP4: Firstly, the interviews with stakeholders in task 4.1 (the relevant results are presented in D.4.4) and, secondly, the analysis of security related future studies. This research-based analysis of needs contained i.e. defining terms, structuring the existing classifications of needs as well as the transfer of these results to the field of security, in particular to cyber infrastructure, nuclear and environment. There are important methodological insights from this analysis which will be transferred to WP3 (see D.4.2 and D.3.2).

The discussion about societal security needs and the additional analysis was extremely useful to identify these needs which were mentioned more frequently across all domains, like *providing information during and after an incident, public communication about risks or maintaining a skilled, knowledgeable workforce.* To summarise the results of the need identification presented in the previous chapter following insights and challenges should be pointed out:

- Deriving the societal security needs was a challenge because of the blurry boundary between needs and solutions in theory as well as in project practice (interviews with stakeholders in the validation workshop). This could result from the specific nature of security being a need itself. The more specific the description of the security need is, the more difficult the distinction between need and solution is. Thus, the concrete need mostly includes solutions. Therefore, the needs stay either at a more abstract level describing issues like the need for protection or they easily end up at a level close to describing solutions like specific types of training measures or technical solutions. In principle, a higher level of description was desired in the analysis, but in some cases there were also more specific needs listed.
- There are also some remarkable insights from the exercise. One is the challenge of ambiguity for which the question of identity in the internet is a good example. While in many cases like disproportion, but also in cases like data trails the protection of anonymity would be seen as an advantage, many other cases show the need for clear identification like vigilantism or cyber mobbing.
- Another challenge was handling the difference in the perception of threats, i.e. the question if a threat is resolvable and how. The answer results in the different level of impact in each scenario.
- Finally, there was the challenge to determine different needs for the different scenarios. In most cases, two, three or even four scenarios showed similar patterns for each domain. In those cases, it was hard to derive different needs. Only in some cases, it was clear that one or two scenarios strongly vary due to the different framework conditions in these

scenarios. However, the impact differs between scenarios and is significantly higher or lower. Based on that assumption, the resulting needs will not vary so much in between the scenarios. There would be more differentiations possible if the likelihood would be also taken into account.

- In the consequence different solutions should be proposed in different scenarios depending on the need intensity.

After the validation workshop, an internal workshop with the consortium members took place in order to summarize the key findings from WP4 and discuss their transfer in particular into WP5. The identified key threats and needs will serve as input for the subsequent WP's (see figure 27). The questions which have to be answered in further analysis are two-fold:

- Firstly, which implications are derived from the different scenarios (e.g. in terms of key critical points, real risks and opportunities)?
- Secondly what can be done to take into account the identified threats and needs and how to take advantage of the identified opportunities?

The scenarios are useful for analysing how different threats impact the society across different plausible futures described in context based threats scenarios. They enable the discussion of different inter-linkages between threats and needs in relation to societal, political, technological and economic issues. These results flow directly in WP5 for evaluating what kind of solutions could be suggested or should be developed to meet these needs in the future. Scenarios provide a framework for prioritising the solutions, which flow directly into WP5: Are they robust towards the different scenarios for one domain? Are they robust towards the different domains?

For the identified needs emerging security opportunities of both a technological and non-technological nature will be proposed in WP5. The first ideas of solutions could be generated, while making concrete the needs. For example a need for a qualified workforce is more concrete, when a specific training packages will be suggested – which might be a possible solution for this need. Furthermore scenarios also point out the possibilities in order to develop a rationale for including or prioritizing research topics in a European strategic security research agenda in WP6.

The critical review of the scenario process will be delivered in D.4.2. These findings will serve as a feedback to WP3 in order to improve the diffusion and awareness of the methodological knowledge.

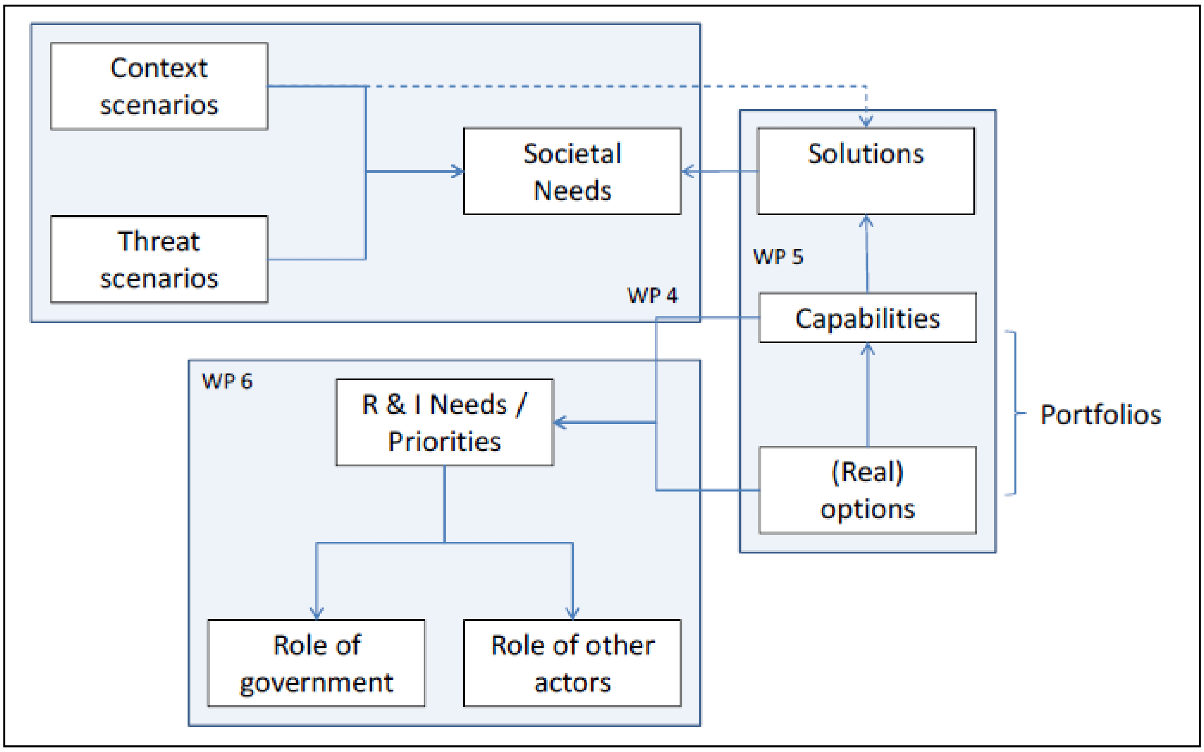
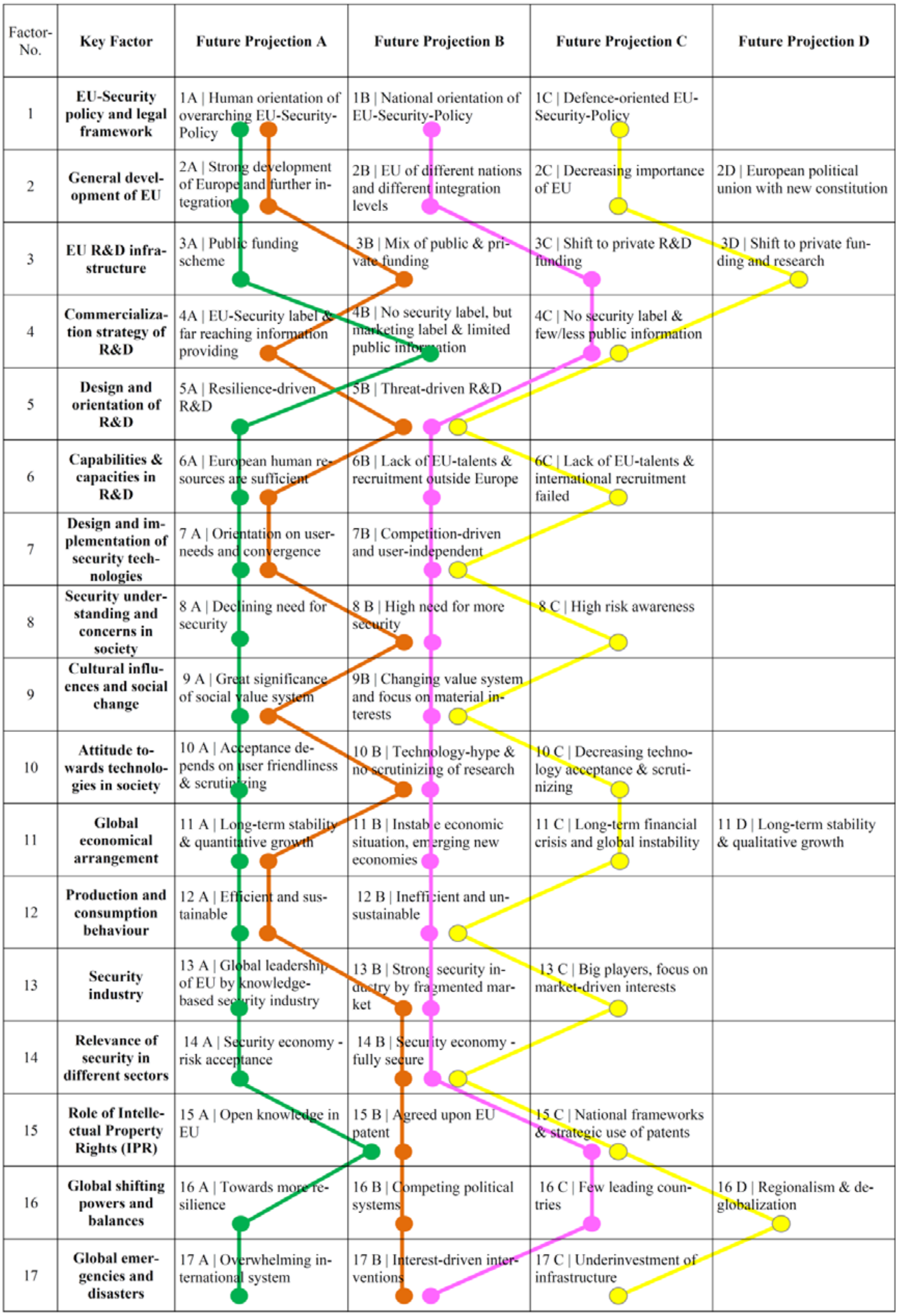


Figure 27: Transfer of the research results from WP4 in WP5 and WP6 (see D.3.1)

4 Appendix

4.1 Context scenarios



Factor-No.	Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
1	EU-Security policy and legal framework	1A | Human orientation of overarching EU-Security-Policy	1B | National orientation of EU-Security-Policy	1C | Defence-oriented EU-Security-Policy	
2	General development of EU	2A | Strong development of Europe and further integration	2B | EU of different nations and different integration levels	2C | Decreasing importance of EU	2D | European political union with new constitution
3	EU R&D infrastructure	3A | Public funding scheme	3B | Mix of public & private funding	3C | Shift to private R&D funding	3D | Shift to private funding and research
4	Commercialization strategy of R&D	4A | EU-Security label & far reaching information providing	4B | No security label, but marketing label & limited public information	4C | No security label & few/less public information	
5	Design and orientation of R&D	5A | Resilience-driven R&D	5B | Threat-driven R&D		
6	Capabilities & capacities in R&D	6A | European human resources are sufficient	6B | Lack of EU-talents & recruitment outside Europe	6C | Lack of EU-talents & international recruitment failed	
7	Design and implementation of security technologies	7 A | Orientation on user-needs and convergence	7B | Competition-driven and user-independent		
8	Security understanding and concerns in society	8 A | Declining need for security	8 B | High need for more security	8 C | High risk awareness	
9	Cultural influences and social change	9 A | Great significance of social value system	9B | Changing value system and focus on material interests		
10	Attitude towards technologies in society	10 A | Acceptance depends on user friendliness & scrutinizing	10 B | Technology-hype & no scrutinizing of research	10 C | Decreasing technology acceptance & scrutinizing	
11	Global economical arrangement	11 A | Long-term stability & quantitative growth	11 B | Instable economic situation, emerging new economies	11 C | Long-term financial crisis and global instability	11 D | Long-term stability & qualitative growth
12	Production and consumption behaviour	12 A | Efficient and sustainable	12 B | Inefficient and unsustainable		
13	Security industry	13 A | Global leadership of EU by knowledge-based security industry	13 B | Strong security industry by fragmented market	13 C | Big players, focus on market-driven interests	
14	Relevance of security in different sectors	14 A | Security economy - risk acceptance	14 B | Security economy - fully secure		
15	Role of Intellectual Property Rights (IPR)	15 A | Open knowledge in EU	15 B | Agreed upon EU patent	15 C | National frameworks & strategic use of patents	
16	Global shifting powers and balances	16 A | Towards more resilience	16 B | Competing political systems	16 C | Few leading countries	16 D | Regionalism & deglobalization
17	Global emergencies and disasters	17 A | Overwhelming international system	17 B | Interest-driven interventions	17 C | Underinvestment of infrastructure	

Figure 28: Four bundles of future projections marked by the coloured lines - basis for context scenarios

4.1.1 “Common wealth” (green path)

In the green scenario big efforts are made towards more resilience and there is an absence of great power conflicts on the global level. The EU is competitive and on the global level there is also a long-term economic stability. There is a strong industrial capability and knowledge base in the security field in Europe. A main focus of the EU is to achieve a worldwide leading position in R&D as well as in security industry. Due to the declining need for security, the risk awareness of the society is sinking. Technology acceptance also differs, depending on its characteristics like suitability for daily use etc. Traditional and social values still remain important in the European countries. Topics like active ageing, life-long education, demographic change and new living models play a significant role.

Stable political and economic framework

The green scenario is mainly driven by the strong EU within a stable global framework. The global scene is marked by economic and political stability in the world, but especially within the EU. Big efforts are made toward more resilience and there is an absence of great power conflicts. As a result of a coordinated global crisis management, global emergencies and disasters can be met effectively and efficiently.

Competitive EU implements security policies

The EU is competitive and on the global level there is also a long-term economical stability. In general, the production and consumption behavior is efficient and sustainable. Within the EU the integration of further states is performing well, also the monetary union has recovered. In addition, the people feel like EU citizens. As a consequence of these positive framework conditions, but also in order to preserve it, the EU makes big efforts in the implementation of overarching security policies, which concentrate on human security, a great cohesion of the EU and the EU enlargement.

Strong European R&D competing with market

A main focus of the EU is to achieve a worldwide leading position in R&D as well as in industry. The EU and national security research show a strong interest in strengthening resilience of the society. Therefore stronger interrelations of European and national research programs are implemented and the EU instruments for supporting R&D cooperation are successful. This also has a positive effect on the job market due to sufficient human resources. Yet, due to the strong market, there is still no security label established by the EU but several market labels exist. Information providing is lead by market and business interests. So design and implementation of security technologies are also oriented on user-needs and convergence. But the acceptance of new technologies still differs depending on use friendliness. The security economy is also oriented towards risk acceptance. The supply and demand for security technologies is decreasing and determined by usefulness.

Sinking risk awareness in society due to peaceful surrounding

Accordingly, the risk awareness of the society is sinking due to the declining need for security. But the meaning of the social value system is important. Although the ‘western’ value system remains important in the European countries, topics like active ageing, life-long education, demographic change and new living models play a significant role. Plus, open knowledge is promoted and the granting of exclusive patents has become rare. The disclosure of information and IP is common. Open Source, Open Data and Crowd Sourcing are prevailing concepts and knowledge is seen as common property. Yet, there is still work done on common standards to enhance security.

4.1.2 “Fortress Europe” (orange path)

The global situation is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive. In the European countries the ‘western’ value system remains important, but there is a strong focus on securitisation of life, pushed forward by the extensive Security Policy of the EU and a fragmented, yet strong security economy and industry. Despite the high technology penetration of everyday life people trust in technological solutions. For higher security level citizens even reduce the claims to their fundamental rights and for high security standards public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

Competing political systems

The worldwide situation is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. Global emergencies and disasters are therefore often used for interest-driven interventions. In the European countries the ‘western’ value system remains important. Yet active ageing, life-long education, demographic change and new living models play a significant role.

Securitisation and harmonisation on EU-Level

On the EU-level harmonisation is far driven, also the enlargement of the EU and the monetary union. An example for harmonisation is the EU security label. The EU Security Policy is human oriented and also concentrated on EU-level, the legal framework is harmonized and a global cooperation to fight terrorism and crime is endeavored. The EU has a strong in raising human security standards, so that the EU represents a location of a common security understanding. Due to the overarching Security Policy, international collaboration on terrorism, crime and cross-border conflicts is performing well.

Stable global economy and strong security industries

The worldwide economy is stable and has reached a level of sustainability, especially the EU is competitive. Yet, the focus is on quantitative growth. The security economy and industry is strong developed but the market is fragmented; especially within the security field there is a strong knowledge base. Security economy is oriented towards fully controllable technologies and aims at achieving a very high security level. As a result, security technologies are everywhere, independently of their usefulness.

Trust in technology and high security levels

Despite the high technology penetration of everyday life people trust in technological solutions. For higher security level citizens even reduce the claims to their fundamental rights and for high security standards public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

Public and private R&D is threat-driven

Due to the strong security industry, the R&D landscape is determined by a mix of pubic and private funding, leading to more competition as well as to an overlap of research. Due to the high level of competition in R&D attractive jobs are offered and European human resources are sufficient. Generally, R&D is mainly threat-driven and oriented on securitisation of life, which makes a dual use of research results – civil and military – possible. As user needs are seen as very important, users are involved in the innovation process.

4.1.3 "Oliver-Twist-Story" (pink path)

The pink scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. There is a strong security industry by a fragmented market. The European security industry is very strong and produces customized security solutions for society. User-friendliness is rather oriented on market interests than on the best solution. There is a high technology penetration of everyday life but also trust in technological solutions. For higher security levels people tend to reduce their rights. In society technologies are seen as a solution for security challenges. Resulting from the economical situation, the society attaches more importance to material interests than to traditional and social values. The social gap grows further and there is a strict differentiation between social classes.

Shifting powers and balances in global politics and economy

The pink scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems, as new powers are emerging. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. When it comes to global emergencies and disasters, interventions are interest-driven, e.g. they are used as a "justification" for military interventions.

Growing social gap, material interests dominate

Generally speaking, the society attaches more importance to material interests than to traditional and social values. The social gap grows further and there is a strict differentiation between social classes (e.g. gated communities). This leads to extreme groups becoming stronger and are difficult to control and to the people's perception that security is more important than freedom.

Minimized EU

The EU is struggling with different topics: It’s political influence is decreasing, the Eurozone is minimized, the EU is characterized by different integration levels. Plus, there is a growing mismatch between local responsibility and European participation. At least the European market is fragmented but strong.

Shift to private funding

As the EU is also not in a position to make considerable investments in R&D, there is a shift to private R&D funding. The EU is hardly capable to make joint decisions. For example, there is also no joint commercialisation strategy of R&D in the EU – neither a security nor a marketing label is established. Another example is the role of IPR, which is dominated by national laws and not by harmonisation on EU-level. Basic research is done less by public institutions, security research is mostly applied research and especially threat driven technology research. There is general shortage of well educated young people in Europe, but the international recruitment is successful as there are attractive jobs offered in Europe.

Threat and market-driven R&D

There is a strong focus on securitisation of life, as private institutions aim to sell their security products. The European R&D structure is also driven by market interests and therefore has a very high innovation speed. This favors a heterogeneous technology landscape which impedes interoperability and standardisation. The society has a minimal impact on the development and innovation process.

Strong security industry

This development enables a strong security industry by a fragmented market. The European security industry is very strong and produces customized security solutions for society. Yet, an overarching dialog between policy makers and security industry is missing. Due to this supply security technologies are everywhere, irrespective of their usefulness.

Need for security enforced by security industry

Further, the security economy is oriented towards fully controllable technologies and wants to achieve a very high security level. This produces an ambivalent technology hype situation: User-friendliness is strongly linked to market interests and not to the best solution. Regarding the concerns of the society, there is interplay between the society’s need for more security and the market- and threat-driven R&D, as well as the instable political situation on the world. Due to the demand of higher security levels, public acceptance is given. Summing up the main points of the pink scenario in the general consumption and production behavior, one might say that it is characterized by inefficiency. The awareness of sustainable consume does exist in the society, but economic aspects are more important.

4.1.4 “Burying heads in the sand” (yellow path)

The worldwide situation is marked by many conflicts. The global political and economic situation is instable and the EU also loses its power. Global powers and balances shift to few regions and there are conflicts over markets. The long-term financial crisis is not overcome. The market is determined by multinational companies and big players which concentrate on markets with few risks. Still US companies dominate the security market. The social gap grows further and there is a strict differentiation between social classes. As an effect of these developments extreme groups become stronger and are difficult to control. The society is aware that not all risks may be covered by security solutions. Technology acceptance is decreasing in general, more effective research is required.

Political conflicts on the global level

In the yellow scenario the global political and economic situation is instable, the EU loses power. The worldwide situation is marked by many conflicts. Global powers and balances shift to few regions and there are conflicts over markets. There is still a long-term financial crisis and growing risk of humanitarian crisis.

Growing social gap and risk acceptance

Resilience has no priority, neither on public nor on private scale. As a consequence the social gap grows further and there is a strict differentiation between social classes, leading to an extensive formation e.g. of gated communities. Another effect of these developments is that extreme groups become stronger and are difficult to control. Because of the persistent instability the society is aware that not all risks may be covered by security solutions.

Strong security industry, controlled by big players

The security industry reacts to the political situation by producing more technologies to achieve a very high security level. The security economy is oriented towards fully controllable technologies which are found everywhere - independently of their usefulness. The market is determined by multinational companies and big players which concentrate markets with few risks. Still, US companies dominate the market. Regarding the design and implementation of security technologies, there is a low influence of the society on technology development and innovation processes. The high level of competition and the heterogeneous technology landscape intensify the innovation speed on the one hand, but impede interoperability and standardisation on the other hand. Accordingly, the production and consumption behavior is inefficient and unsustainable.

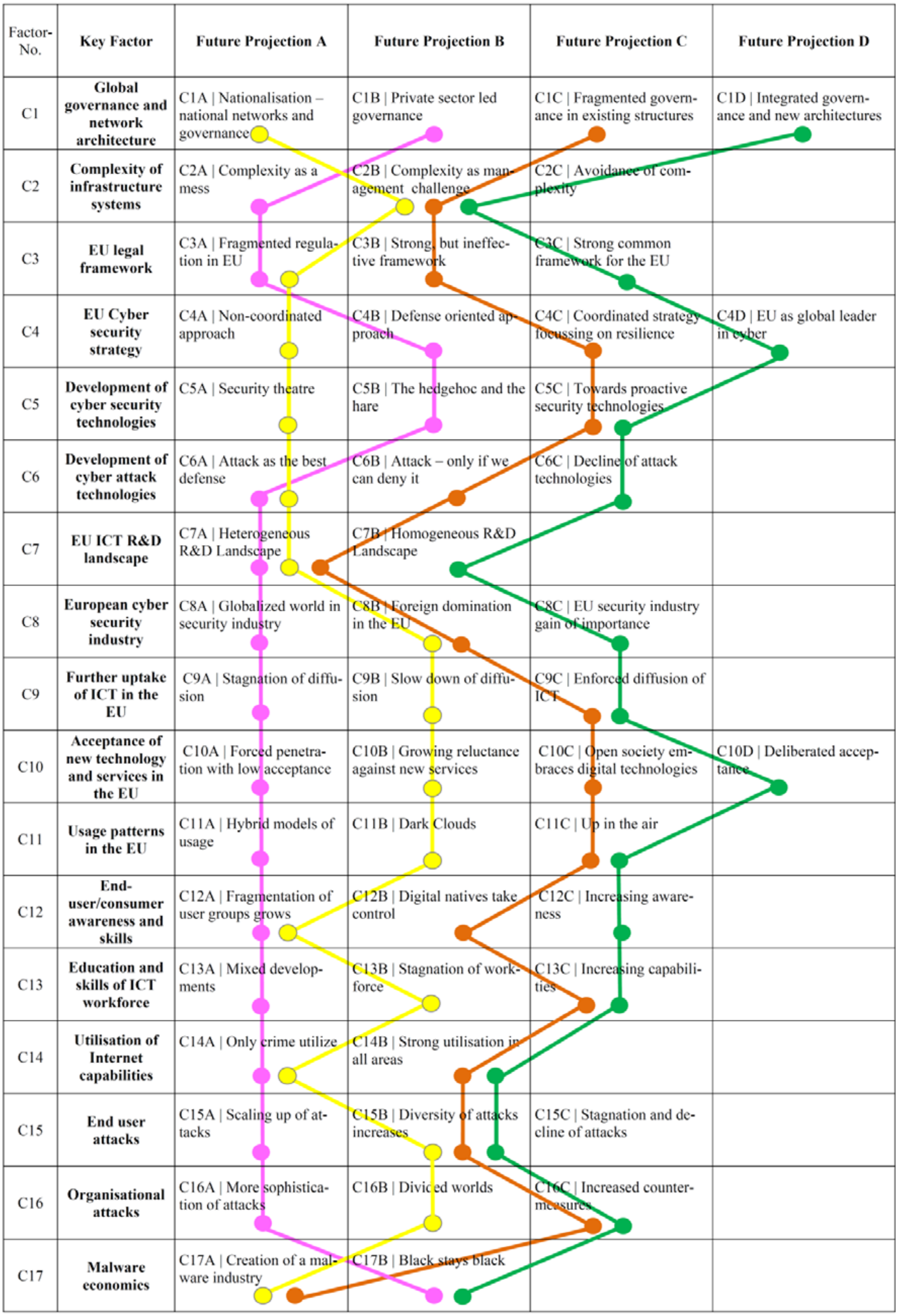
Weak EU, collaboration only on security issues

Within the EU the states turn back to their own national interests and further enlargement and integration of the EU is given up. Also the EU has a minimal influence on (national) legal frameworks. Citizens even don’t feel like EU citizens any more. At least, there is still cooperation on EU level in terms of a defense-oriented EU-security policy, yet there is a strong focus on national and international security.

Insufficient and ineffective R&D

Since joint R&D activities are cut back within the EU, there is a shift to private funding within the R&D landscape. As a result, patents are used as strategic instruments as the member states of the EU even do not agree upon a common EU patent. Security research is mostly applied research and basic research is insufficient. Due to these cuts there is a general shortage of well educated, talented young people within the EU. Being led by the interests of private institutes and their market interests, R&D is mostly threat-driven and likewise security research is threat-driven technology research.

4.2 Cyber infrastructure scenarios



Factor-No.	Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
C1	**Global governance and network architecture**	C1A | Nationalisation – national networks and governance	C1B | Private sector led governance	C1C | Fragmented governance in existing structures	C1D | Integrated governance and new architectures
C2	**Complexity of infrastructure systems**	C2A | Complexity as a mess	C2B | Complexity as management challenge	C2C | Avoidance of complexity	
C3	**EU legal framework**	C3A | Fragmented regulation in EU	C3B | Strong, but ineffective framework	C3C | Strong common framework for the EU	
C4	**EU Cyber security strategy**	C4A | Non-coordinated approach	C4B | Defense oriented approach	C4C | Coordinated strategy focussing on resilience	C4D | EU as global leader in cyber
C5	**Development of cyber security technologies**	C5A | Security theatre	C5B | The hedgehoc and the hare	C5C | Towards proactive security technologies	
C6	**Development of cyber attack technologies**	C6A | Attack as the best defense	C6B | Attack – only if we can deny it	C6C | Decline of attack technologies	
C7	**EU ICT R&D landscape**	C7A | Heterogeneous R&D Landscape	C7B | Homogeneous R&D Landscape		
C8	**European cyber security industry**	C8A | Globalized world in security industry	C8B | Foreign domination in the EU	C8C | EU security industry gain of importance	
C9	**Further uptake of ICT in the EU**	C9A | Stagnation of diffusion	C9B | Slow down of diffusion	C9C | Enforced diffusion of ICT	
C10	**Acceptance of new technology and services in the EU**	C10A | Forced penetration with low acceptance	C10B | Growing reluctance against new services	C10C | Open society embraces digital technologies	C10D | Deliberated acceptance
C11	**Usage patterns in the EU**	C11A | Hybrid models of usage	C11B | Dark Clouds	C11C | Up in the air	
C12	**End-user/consumer awareness and skills**	C12A | Fragmentation of user groups grows	C12B | Digital natives take control	C12C | Increasing awareness	
C13	**Education and skills of ICT workforce**	C13A | Mixed developments	C13B | Stagnation of workforce	C13C | Increasing capabilities	
C14	**Utilisation of Internet capabilities**	C14A | Only crime utilize	C14B | Strong utilisation in all areas		
C15	**End user attacks**	C15A | Scaling up of attacks	C15B | Diversity of attacks increases	C15C | Stagnation and decline of attacks	
C16	**Organisational attacks**	C16A | More sophistication of attacks	C16B | Divided worlds	C16C | Increased countermeasures	
C17	**Malware economics**	C17A | Creation of a malware industry	C17B | Black stays black		

Figure 29: Four bundles of future projections marked by the coloured lines - basis for cyber scenarios

4.2.1 “Good new cyber world” (green path)

In the green context scenario big efforts are made towards more resilience and there is an absence of great power conflicts on the global level. The EU is competitive and on the global level there is also a long-term economic stability. There is a strong industrial capability and knowledge base in the security field in Europe. A main focus of the EU is to achieve a worldwide leading position in R&D as well as in security industry. Due to the declining need for security, the risk awareness of the society is sinking. Technology acceptance also differs, depending on its characteristics like suitability for daily use etc. Traditional and social values still remain important in the European countries. Topics like active ageing, life-long education, demographic change and new living models play a significant role.

Strong international internet governance and cooperation

In this scenario an ***integrated global governance of the internet*** through widely respected public bodies enables the introduction of ***new network architectures*** based on security principles and interoperability aimed to improve the situation compared to today. Moreover it also leads to further integrated developments like ***strong international collaborations*** in the prevention and prosecution of cyber crime and cyber terrorism as well as official ban of cyber warfare. Consequently the development of attack technologies declines and most countries use them only for research purpose. Only a few countries do not follow this track. While attacks only play very limited part in this, cyber espionage is one of the emerging topics.

Harmonized and integrated EU cyber policy

Based on a ***strong and future oriented common framework*** coordinating all relevant aspects like data protection and privacy, digital consumer rights, cyber crime prosecution and a real digital single market enabled by powerful EU institutions ensuring the necessary cooperation, the EU is one driving force of this development. Consequently the EU also takes a/the ***leading role in cyber security*** by the means of strong public-private partnerships or/and standardisation efforts in the cyber security area. Overall the framework and the cyber security strategy are aimed at balanced mixture of prevention and prosecution. This goes along with a strong ***focus on developing cyber security technologies***, which is based on an increase of public and private investments and their effective coordination as well as involvement of relevant experts from all fields. The focus of the research shifts more and more towards proactive security technologies aimed at prevention of cyber security incidents. Progress in this direction is based amongst other things on autonomous technologies and advances in cryptography as well as increased orientation towards aspects like user friendliness. As a consequence the ***EU security industry gains of importance*** in the field of cyber security and become an important global player in this domain based on collaborations between the industries in the member states. This is achieved by increasing the capabilities of the EU to respond to threats in cyber security based on their own industry.

Massive and deliberative adoption and acceptance of ICT by all and in all spheres

The strong role of Europe goes along with an ***enforced diffusion of ICT*** into both, business as well as private everyday life. It is based on high bandwidth access for all and the diffusion of new technologies such as the internet of things and of services, which also result into an increased digitalisation of process in business and public services. Consequently the uptake of Cloud Computing will gain importance and more and more ***cloud services are used by all***, business, public authorities and consumers, because, due to high security standards and competitive markets, the usage of such services are of benefit for many different users. At the same time the acceptance of ICT and in particular new ICT technologies is shaped by a ***well-balanced perception of challenges and chances*** leading to conscious use of technologies, i.e. use of specific trusted services and tools. This is a result of the growing efforts to increase the consumer and end user skills and awareness regarding cyber threats. Though it succeeds it is based on massive public efforts and despite these efforts some are still left behind. This public effort is complemented by the/a strategy to ***increase the number and quality of education of the ICT workforce*** in Europe. Measures are on the one side the targeted inclusion of women or elderly workforce and on the other side strong focus on usability as well as lifelong learning strategies. One side effect is that the growing needs of the strong European cyber security industry can be also satisfied. Another consequence of this overall development is the ***growing entanglement of different infrastructures***, e.g. energy, transportation, leading into an increased importance of the cyber infrastructures. However the resulting ***complexity of the systems are seen and approached as management problem*** by clear policies like upgrading legacy systems or strict guidelines based on a better education.

Level of cyber threats varies strongly

Regarding the threat level there are some diverse developments. On the one hand ***cyber crime and terrorism become even more prosecuted*** due to the strong cooperation and new technologies. This goes along with a clear ethic for all others to publish, not to sell cyber security exploits, which is enforced by a supplementing open policy of the industry. Nevertheless, the number of attacks still increases, not only in numbers, but also in their diversity. ***Advances in security technology*** lead to higher security standards in public institutions and business. Consequently the risk of detection and prosecution in this area increases. But because of this decreases the reward/risk ratio cyber criminals focus more on consumers. Here the security landscape varies strongly and because of that the number of attacks is increasing. While most of the simple and unspecified attacks aimed at fraud or thievery fail more and more, there is also a ***trend to more targeted attacks*** on specific user groups that is still very successful. Nevertheless, ***the risks of detection and prosecution of cyber crime and cyber terrorism increases*** in general, due to the strong utilisation of resources and advances in security technology. In addition the consequences in terms of fines and penalties are more and more established and utilized.

4.2.2 “Almost open” (orange path)

The global situation in this context scenario is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive. In the European countries the ‘western’ value system remains important, but there is a strong focus on securitisation of life, pushed forward by the extensive Security Policy of the EU and a fragmented, yet strong security economy and industry. Despite the high technology penetration of everyday life, people trust in technological solutions. For higher security level citizens even reduce the claims to their fundamental rights and for high security standards public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

Diverse international internet governance in existing structures

Overall this scenario is shaped by a strong diversity where existing structures and fundamental changes exist beside each other. One clear point is that the global governance will be still based of the already ***existing governance structures and architecture principles*** resulting into limited and partly problematic international cooperation against cyber crime and terrorism. There are also no advances in developing new overarching secure frameworks. Another ambiguity is that ***cyber warfare is now regulated*** like other ways of warfare. Nevertheless, many countries preparing themselves for cyber warfare by developing offensive capacities, but due to the official regulations this takes place behind the walls of secret public institutions. This offers the possibility to ***deny such activities***.

Strong and coordinated, but ineffective EU cyber policy

Within this environment the EU pursues a coordinated ***cyber strategy focused on resilience*** through a coordination of public and private efforts as well as inclusion of citizens, strong focus on human rights and a broad definition of cyber security. However this strategy remains most likely a toothless tiger, because the ***resulting EU wide legal framework seems to be strong, but proves to be ineffective*** in reality. Reasons are that it tends on the one hand towards overregulation with too many, partly contradictive regulations. On the other hand some fundamental objectives were undermined by strong industrial lobbies. Finally the high expectations on the strategy and framework failed and people are disappointed. However due to the ambitious approach of the cyber security strategy, there is a clear ***shift towards proactive security technologies*** focusing on prevention and early detection. It is based on many progressive technologies like autonomous systems and enhanced cryptographic technologies, but due to the heterogeneous R&D landscape it lead also to very diverse results. The lack of stable, public investments in research, the resulting low business expenditure for R&D and the lack of coordination between EU and its member states lead to many doublings and wasted efforts in R&D. Consequently the ***market for cyber security technologies is still dominated by foreign, most likely by US player***. Therefore the EU is still relying on foreign suppliers, while EU companies only act in niches.

Further diffusion of ICT forced by digital natives

Contrasting to this there is an ***increased diffusion of ICT*** in all spheres of society and business. This includes the breakthrough of the Internet of services and things that lead to a growing connection of infrastructures ***boosting the importance of cyber infrastructures***. This is mainly based on the availability of broadband, but also on the fact that an open society with many digital natives is open towards emerging digital technologies, i.e. have a basic strong trust in the internet and the used measures to ensure this due to openness as a basic principle. One reason is that the ***digital natives*** are used to digital technologies and therefore in general are more aware of challenges and risks, but in some cases they are also careless, due to the strong trust in technology, so that risk avoidance is not the guiding principle. This overall situation also leads to a fast uptake of new services. In particular ***cloud services will be adapted in massive style*** by all, consumers, public services as well as business, because of its overall benefits for most users. Moreover the wish towards openness and the growing experience of digital natives lead to the fact that the industry sees high security as a competitive advantage in a highly competitive market. The ***growth of user experiences*** goes hand in hand with ***a better skilled ICT workforce***, which is also growing in numbers. This is also one reason for the growing complexity of the infrastructure systems because of interrelations are seen and approached as management problem by clear policies like upgrading legacy systems or strict guidelines based on a better education.

Ambiguity in the cyber threat level

While attacks on ***institutional targets provoke clear countermeasures*** passed on general progress in advanced cyber security technologies in Europe and the rest of the world, the situation for consumers differ. While the more and more experienced digital natives are better prepared for simple mass attacks of cyber crime such as phishing, which still increase in number because of their decreasing efficiency, all ***consumer are still very likely to become victim*** of more specific targeted cyber crimes. One reason for this is that the ***grey zone of cyber war***, where specialized public agencies and hackers create a kind of shadow system for such attacks, is evolving. Officially as an act of defense they start to buy software exploits, which lead into new patterns for hackers where to sell is better as to tell, at least for some of them. Another reason for the growing risks in particular for consumers is that the ***development of efficient countermeasures fail***, which is partly also a result of a failed cyber security strategy and its consequences. While it does not prevent crime or terrorism, there is still a strong effort in the prosecution of it by exploiting the potentials of the internet itself like massive data retention. Especially terrorism and crime against institutions is seen as a major risk and there is strong and balanced systems of fines and penalties established. In case of crime against consumers the results are more ambiguous, because though the risk of detection and punishment may increase, there is still a good chance to get away with it.

4.2.3 "Going private" (pink path)

The pink context scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. There is a strong security industry by a fragmented market. The European security industry is very strong and produces customized security solutions for society. User-friendliness is rather oriented on market interests than on the best solution. There is a high technology penetration of everyday life but also trust in technological solutions. For higher security levels people tend to reduce their rights. In society technologies are seen as a solution for security challenges. Resulting from the economical situation, the society attaches more importance to material interests than to traditional and social values. The social gap grows further and there is a strict differentiation between social classes.

Industry driven internet governance

On a global level the governance and architecture of the cyber infrastructure are taken over by ***private organized bodies***, which will introduce new architectural concepts mainly based on ***market driven approaches***, i.e. forced by industrial consortia and players. Due to this dominance the international cooperation will be focused more on cyber crime then on cyber terrorism. Moreover there are strong private driven activities like commercial espionage, which might have an influence on the development of the global governance framework, i.e. the institutional development of governance structure, in particular ones driven by public actors, will be thwarted.

Defense driven EU cyber policy

In Europe the cyber security strategy on the level of the EU as well as on member state level is strongly focused on a ***defense driven approach***, i.e. it will focus on securing critical issues, but less on human rights or an inclusion of civil society resulting into a ***neglection of societal dimensions of security***. This goes along with the fact that the regulatory landscape in Europe is shaped by fragmentation. In particular the legislations on privacy or consumer rights differ strongly due to the different influence of private led interests groups in different member states. Consequently there are only few unified regulations across Europe as well as a ***low level of cooperation*** between the states. Against this background the research and development in science and technology will show some clear patterns. Due to the fact that many national strategies see attack as an integral part, which is a result of the remaining insecurities, the ***development of cyber attack technologies will pushed forward*** by strategic research agendas as well by the creation of specialized institutions. This development is clearly taken-up by the industry and will lead to a bloom of specific companies focusing on attack technologies. Moreover it also creates a ***grey market between industry and specific types of hackers***, where exploits will be sold, not made public. In the long run this will undermine security efforts led by civil organisations based on openness. The strong focus on attack technologies will also lead to a neglect of the development of security technologies. This results in a situation, where only security solutions for big companies are developed, while consumers and small companies lack of appropriate solutions. Consequently ***security technology will always be behind*** and is less focused on user concerns or prevention, but more detection and forensic of attacks. This situation will be aggravated by the fact that the R&D landscape suffers under low public investment with a lack of coordination and cooperation between the member states in the EU. Consequently R&D investments are driven by the industry and directed in areas where the expected profit is maximized. However the strong international competition of industrial consortia, in particular also from emerging countries, will, in conjunction with the nationalisation tendency and efforts to build national champions, lead to the effect that the ***US dominance in the cyber security market will end***, partly also because of exclusion in critical areas.

Forced diffusion with growing reluctance

In this environment the further diffusion of ICT technologies begins to stagnate. As a reaction business and public institutions will start to ***force the further penetration***, at least in selected areas and sectors. As a reaction on this forced development a further ***decrease in acceptance of new technologies*** will take place, which in the long run may affect the development badly. First signs of it will be that the diffusion and adaption patterns will start to vary leading to fragmentation of users into very experienced and growing numbers of left-behinds. Together with the private driven international governance both developments will lead to a situation where the uptake of new technologies like IPv6 or the Internet of things and services vary strongly in the different countries. Only in some areas it will take up, while others stay at the level of older technologies. This goes along with slower development of connectivity, in particular in the consumer area, which is another barrier for the uptake of new services in the EU. While the entanglement of infrastructures is also in the focus of business and public services, the consequences of it will not be considered. Problems such as legacy systems or the faster IT lifecycles are not reflected carefully. Another point influencing the uptake of services like cloud computing is that the ***fragmentation into very different user groups*** will lead to a situation where the usage of such services will not obviously offer benefits for all, but at least for the majority. Consequently private business and public services will force a strong adoption. This diverse development of the users side is also reflected in the development of the ICT workforce, where ***the number in total may increase, but the quality strongly varies***, i.e. only few manage to hold on with the speed of the technological development. Consequently there will be an ongoing fight for the best talents, in particular in the industry.

Rising threat level in cyber

The fragmentation of the legal framework as well as other factors going along with it like the lack of cooperation, lack of effective measures for prosecution and prevention, the focus on attack technologies will lead to an ***increased threat level*** for both, consumers as well as for business and public services. Exploiting the vulnerabilities as well as the capabilities of the internet ***enables cyber crime to scale up their attacks*** on consumers by increasing the number as well as the quality of attacks resulting in a higher risk to become victim for consumers. This will be made worse by insufficient security solutions for consumers. But not only consumers, ***also business and public administration become more and more targets*** of sophisticated attacks. These are not only directed at cyber crime, but also shaped by an intensified commercial espionage and related activities as well as more complex crimes like cyber extortion.

4.2.4 "Fragmented world" (yellow path)

The worldwide situation is marked by many conflicts. The global political and economic situation is instable and the EU also loses its power. Global powers and balances shift to few regions and there are conflicts over markets. The long-term financial crisis is not overcome. The market is determined by multinational companies and big players which concentrate on markets with few risks. Still, US companies dominate the security market. The social gap grows further and there is a strict differentiation between social classes. As an effect of these developments extreme groups become stronger and are difficult to control. The society is aware that not all risks may be covered by security solutions. Technology acceptance is decreasing in general, more effective research is required.

Nationalisation of internet governance

Overall this scenario is driven by a strong fragmentation above all dimensions. On a global level the ***governance and architecture of cyber infrastructures is driven by a gradual nationalisation***. Many, maybe all countries try to install national governance structures in order to keep control on the development of the internet. While this development started more in autocratic regimes, it will lead to a growing number of nations trying to create their own secure single islands. Consequently there is only ***low level on international cooperation*** on cyber crime and terrorism and subsequently no regulation on cyber war between the nations.

Non-coordinated cyber policy in the EU

In the course of this the development within in the EU is also shaped by a ***non-coordinated-approach in regard to the cyber security strategy and a fragmented regulation landscape***. While some of the member states may try to force increased cooperation, others insist on their national interest. Overall this will lead to a separation in important questions and a ***lower level of cooperation*** between the EU and its member states. Moreover most nations will pursue in the aftermath different approaches towards national strategies with different threat definitions and strategy development processes. Finally this will lead into in a very fragmented legislation on major points like data protection or cross-border operations. ***The technological development is shaped by ambiguous developments***. At a first glance both areas, security as well as attack technologies, experience a strong growth, but in detail there are strong differences. While in the case of cyber security, a technology which is mostly driven by national players, lead to forced development, it turns out that the benefits of it are unclear. The reason for this is that users can't act on them and experience difficulties to integrate it in their normal usage and work. Similar to it the development of attack technologies is also pushed forward as a consequence of the fact that attack capabilities are seen often as an essential part of national cyber security strategies. In total these both developments lead to much technological advancement, but due to the factor that there is no clear coordination many double efforts are undertaken within the EU member states and possible synergies will be not used because of security reasons. This situation will sustain the current ***dominance of foreign industry players***, in particular the ones from the US because of their strong foothold in the EU. Only in some niche markets the national effort lead to the creation of EU companies as global players. As a consequence of this whole development ***much insecurity about the reliability of security solutions will remain***.

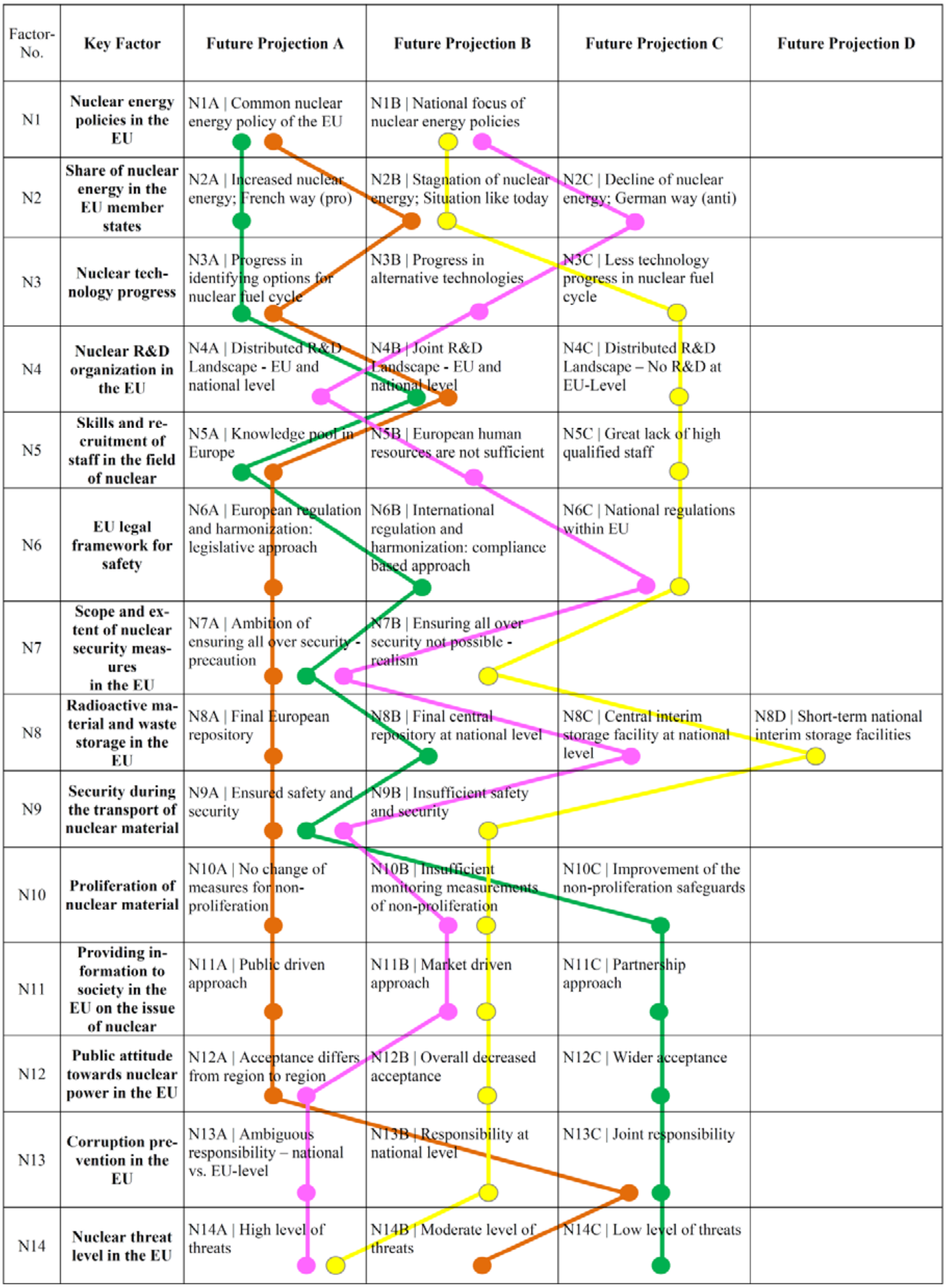
Growing reluctance and slowdown of diffusion

In this environment the further diffusion of ICT technologies is ***shaped by a growing reluctance***, in particular of consumers and end-users. This will lead to a growing distrust in new services and subsequently a ***slowdown of the diffusion of ICT***. It goes along with a general decrease in acceptance of new technologies, which in the long run may affect the development badly. First signs of it will be that the ***diffusion and adaption patterns will start to vary*** leading to delayed adoption of technologies such as IPv6 or internet of things in Europe. Most likely the adoption patterns will vary between sectors and industries as well as between regions in the EU. Based on that one major point is that cyber infrastructures will gain only slowly of importance, because the entanglement with other infrastructures like energy or transportation is driven by a preference of risk avoidance, i.e. too much complexity is seen as critical fact and therefore only punctual connections are preferred. Another point influencing the uptake of services like cloud computing is that the ***fragmentation into very different user groups*** will lead to a situation where the usage of such services will not obviously offer benefits for all. Consequently there will be a selected group which uses the cloud and similar extensively, while most of the consumers avoid it due to insecurities and a growing reluctance against new services. This diverse development of the users is also reflected in the development of the ICT workforce, which will grow, but not fast enough to deal with the growing needs of the industry and society in Europe.

Overall threat level increase

Based on the growing nationalisation, which result in a ***lack of international cooperation and effective measures for prevention and prosecution***, the threat level will increase. This, on the hand, prevents a strong utilisation of the internet for prosecution. On the other hand cyber crime and terrorism, but also espionage and related activities will not stop because of national governance structures. Rather, it ***will lower the risk of detection and prosecution*** and subsequently gives a new push towards more attacks. However, due to the growing user reluctance, the known mass attacks on consumer will loose of efficiency. They will be replaced by specified attacks, which will hit unprepared consumers directly. A similar pattern will be seen in business and public services. While a few resourceful institutions are able to protect themselves quite well, others, in particular small and medium sized enterprises, will be increasingly targets of successful attacks. This development is also a consequence of the ***emerging malware industry***, where the efforts to develop attack technologies lead into new behavioural patterns preventing companies and hackers to publish known exploits. In particular the latter will strongly benefit if they sell it to interested parties.

4.3 Nuclear scenarios



Factor-No.	Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
N1	**Nuclear energy policies in the EU**	N1A | Common nuclear energy policy of the EU	N1B | National focus of nuclear energy policies		
N2	**Share of nuclear energy in the EU member states**	N2A | Increased nuclear energy; French way (pro)	N2B | Stagnation of nuclear energy; Situation like today	N2C | Decline of nuclear energy; German way (anti)	
N3	**Nuclear technology progress**	N3A | Progress in identifying options for nuclear fuel cycle	N3B | Progress in alternative technologies	N3C | Less technology progress in nuclear fuel cycle	
N4	**Nuclear R&D organization in the EU**	N4A | Distributed R&D Landscape - EU and national level	N4B | Joint R&D Landscape - EU and national level	N4C | Distributed R&D Landscape – No R&D at EU-Level	
N5	**Skills and recruitment of staff in the field of nuclear**	N5A | Knowledge pool in Europe	N5B | European human resources are not sufficient	N5C | Great lack of high qualified staff	
N6	**EU legal framework for safety**	N6A | European regulation and harmonization: legislative approach	N6B | International regulation and harmonization: compliance based approach	N6C | National regulations within EU	
N7	**Scope and extent of nuclear security measures in the EU**	N7A | Ambition of ensuring all over security - precaution	N7B | Ensuring all over security not possible - realism		
N8	**Radioactive material and waste storage in the EU**	N8A | Final European repository	N8B | Final central repository at national level	N8C | Central interim storage facility at national level	N8D | Short-term national interim storage facilities
N9	**Security during the transport of nuclear material**	N9A | Ensured safety and security	N9B | Insufficient safety and security		
N10	**Proliferation of nuclear material**	N10A | No change of measures for non-proliferation	N10B | Insufficient monitoring measurements of non-proliferation	N10C | Improvement of the non-proliferation safeguards	
N11	**Providing information to society in the EU on the issue of nuclear**	N11A | Public driven approach	N11B | Market driven approach	N11C | Partnership approach	
N12	**Public attitude towards nuclear power in the EU**	N12A | Acceptance differs from region to region	N12B | Overall decreased acceptance	N12C | Wider acceptance	
N13	**Corruption prevention in the EU**	N13A | Ambiguous responsibility – national vs. EU-level	N13B | Responsibility at national level	N13C | Joint responsibility	
N14	**Nuclear threat level in the EU**	N14A | High level of threats	N14B | Moderate level of threats	N14C | Low level of threats	

Figure 30: Four bundles of future projections marked by the coloured lines - basis for nuclear scenarios

4.3.1 “Greening the image” (green path)

In the green context scenario big efforts are made towards more resilience and there is an absence of great power conflicts on the global level. The EU is competitive and on the global level there is also a long-term economic stability. There is a strong industrial capability and knowledge base in the security field in Europe. A main focus of the EU is to achieve a worldwide leading position in R&D as well as in security industry. Due to the declining need for security, the risk awareness of the society is sinking. Technology acceptance also differs, depending on its characteristics like suitability for daily use etc. Traditional and social values still remain important in the European countries. Topics like active ageing, life-long education, demographic change and new living models play a significant role.

Harmonisation and regulation of EU nuclear energy policy

The EU has a common nuclear energy policy. There is a high interaction between nuclear energy policy, security policy and other policy areas, like environmental policy or fiscal and financial policies. The international regulation and harmonisation of the legal framework for safety is achieved. It based on compliance with regulations (instead the obligation), thus legislation is based on consultation with experts from science and industry as well as public consultation. There is a good base for the joint waste management in a European centralized geological repository (or few repositories) with joint financing scheme (member states and EU).

Precaution in global handling of nuclear sector

Based on lessons learned from previous actions or incidents there is ambition to cover all (thinkable) nuclear threats (precaution). The appropriate solutions are in place. One example is the ensured safety and security during the transport of nuclear material due to the regulated and structured transport with joint responsibility and integration of different stakeholder and experts. More countries joined the Nuclear Non-proliferation Treaty (NPT) and renounced nuclear weapons to enhance national security. The non-proliferation safeguards were improved, like diversion of nuclear material, which should be declared.

Growing acceptance of nuclear power

The far reaching information providing to society with public and private responsibility and the high importance of security culture (e.g. measures for education and training) lead to a wider acceptance of the nuclear power in the EU. Society is directly involved in decisions about the nuclear power, policy or construction of underground disposal sites (or indirectly by representatives). There is more trust in institutions, which provide information.

Progression in nuclear energy and increased share

The share of the nuclear energy increased, based on acknowledgement of the benefits of the use of nuclear energy, like diversification of energy supply, reducing dependence on oil and producing fewer greenhouse gas emissions. Another reason for this growth are new solutions for sustainable fuel cycle, like reducing waste due to improving resource utilisation (recycling and reuse of uranium and plutonium) as well as integrating theory and experiment with modelling and simulation. This technology progress is enabled by a joint R&D Landscape at EU and national level as well as an involvement of policy makers and industry as necessary partners in

R&D. In Europe technological, industrial and scientific competences have high standards and attractive jobs for nuclear scientific are offered.

4.3.2 “High-security structures” (orange path)

The global situation in this context scenario is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive. In the European countries the ‘western’ value system remains important, but there is a strong focus on securitisation of life, pushed forward by the extensive Security Policy of the EU and a fragmented, yet strong security economy and industry. Despite the high technology penetration of everyday life, people trust in technological solutions. For higher security level, citizens even reduce the claims to their fundamental rights and for high security standards public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

Nuclear power not competitive, yet regulated in EU

The nuclear power is still not competitive compared to other energy types, like coal or natural gas and doesn´t make a significant difference in carbon dioxide emissions. This leads to the stagnation of nuclear energy in the EU. However there are still countries in the EU, which own the nuclear power plants. They cooperate with each other and have joint solutions for nuclear energy policy. There is a high interaction between nuclear energy policy, security policy and other policy areas, like environmental policy or fiscal and financial policies as well as a legislative approach and advanced European harmonisation and regulation, yet structures for compliance are missing. The most countries have one final repository underground as an efficient solution at national level.

Different policy-strategies in EU-states with or without nuclear power

In the EU member states with nuclear power are policy makers as well as the industry involved in R&D as necessary partners. Europe has technological, industrial and scientific competences according the nuclear power plants and joint R&D landscape in the field of nuclear material. In countries with nuclear power attractive jobs are offered. On this basis more solutions for sustainable fuel cycle were developed, like reducing waste due to improving resource utilisation (recycling and reuse of uranium and plutonium) as well as integrating theory and experiment with modelling and simulation.

Precaution in EU-standards but no global agreements

The strong focus on securitisation of life leads to an ambition to cover all (thinkable) nuclear threats (precaution). The solutions based on lessons learned from previous actions or incidents. The safety and security during the transport of nuclear material is ensured due to the regulated and structured transport with joint responsibility and integration of different stakeholder and experts. However there is no change of measures for non-proliferation as well as no extension of the Nuclear Non-Proliferation Treaty (NPT) to further nuclear states. There is still no obvious diversion of nuclear material and there are undeclared nuclear materials or activities in the states concerned.

Information provided interest-driven

The far reaching, but interest driven information providing, driven by country policies or policies of the EU, especially by those with nuclear energy result in different acceptance between EU regions (or member states) with higher level of support for nuclear energy in EU nuclear countries compared to EU non-nuclear countries.

4.3.3 "Losing significance" (pink path)

The pink context scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. There is a strong European security industry by a fragmented market. The security industry produces customized security solutions for society. User-friendliness is rather oriented on market interests than on the best solution. There is a high technology penetration of everyday life but also trust in technological solutions. For higher security levels people tend to reduce their rights. In society technologies are seen as a solution for security challenges. Resulting from the economical situation, the society attaches more importance to material interests than to traditional and social values. The social gap grows further and there is a strict differentiation between social classes.

Missing long-term EU-strategy and declining share of nuclear energy

No significant investments made to improve the power plants in many European countries, while the existing reactors are going to retire (high cost of shutting down) and lack of assistance programs on the European or national level lead to declined share of nuclear energy in the EU. The nuclear energy policies have rather a national focus and there is no framework or agreed strategic approach as well as real long term strategic thinking (100y+) at EU-level.

Underinvestment in nuclear energy, concentration on alternative technologies

There is a small community of nuclear experts with focus on core research fields, like nuclear waste management, but in generally the European human resources are not sufficient. This situation as well as underinvestment of R&D infrastructure in nuclear science and less synergies between stakeholders at EU and national level result in no technology progress in nuclear fuel cycle. However there is a breakthrough in nuclear alternative technologies (like Fusion, solar, fracking) instead.

Ineffective international agreements and short-term national solutions

There are still no solutions for a final repository, however there are central interim storage facilities at national level with rather public responsibility. Safety regulation is carried out at national level by national regulatory agencies, which differ between member states. The international commitments are practically not effective, because of the lack of compliance and sanctions. The monitoring measurements of non-proliferation are insufficient due to difficulties of enforcing international treaty obligations and widespread use of nuclear technologies in countries with very diverse systems.

Risk-aware society, but interest-driven information providing

There is an ambition to cover all (thinkable) nuclear threats in society, like to guarantee the safety and security during the transport of nuclear material. This is ensured due to the regulated and structured transport with joint responsibility and integration of different stakeholder and experts. Providing nuclear related information, i.e. about nuclear risk is lead by market and business interests, thus the information is limited. For that reason the acceptance differs between EU regions (or member states) with higher level of support for nuclear energy in EU nuclear countries compared to EU non-nuclear countries.

4.3.4 “Losing acceptance” (yellow path)

The worldwide situation is marked by many conflicts. The global political and economic situation is instable and the EU also loses its power. Global powers and balances shift to few regions and there are conflicts over markets. The long-term financial crisis is not overcome. The market is determined by multinational companies and big players which concentrate on markets with few risks. Still US companies dominate the security market. The social gap grows further and there is a strict differentiation between social classes. As an effect of these developments extreme groups become stronger and are difficult to control. The society is aware that not all risks may be covered by security solutions. Technology acceptance is decreasing in general, more effective research is required.

Focus on national interests without long-term decisions

Thus the EU loses its power, there is a national focus of nuclear energy policies with no framework or agreed strategic approach as well as real long term strategic thinking (100y+) at EU-level. The distributed nuclear R&D landscape with investments of R&D infrastructure driven by national interests as well as a general shortage of well educated, talented young nuclear experts result in insufficient development of sustainable technologies which reduce waste due to improved resource utilisation (recycling and reuse of uranium and plutonium). There is no long-term prognosis for behaviour of the radioactive material of the castor storage.

No problem-solving; stagnating share of nuclear energy

This situation leads to the stagnation of the share of the nuclear energy, thus the nuclear power is still not competitive compared to other energy types, like coal or natural gas and doesn´t make a significant difference in carbon dioxide emissions. There are still short-term solutions for interim storage facilities at the national level, thus sites with low local resistance are preferred over those with best geological conditions. There is also a confusion concerning the responsibility for disposal: private (in nuclear power plants) vs. public (elsewhere).

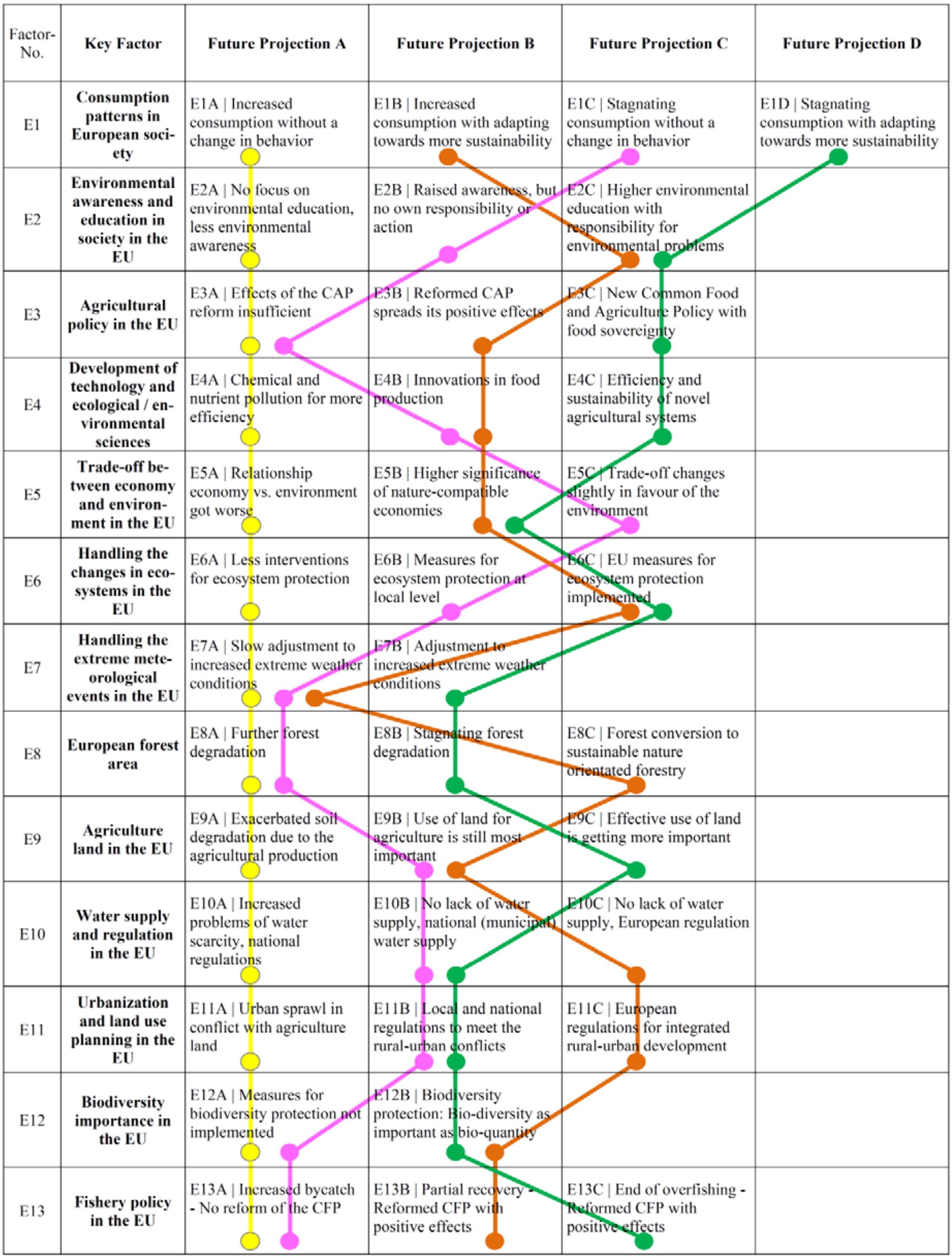
No agreements on international level

Safety regulation is carried out at national level by national regulatory agencies, which differ between member states. The international commitments are practically not effective, because of the lack of compliance and sanctions. The monitoring measurements of non-proliferation are insufficient due to difficulties of enforcing international treaty obligations and widespread use of nuclear technologies in countries with very diverse systems. Therefore the safety and security over the radioactive waste during transport has not is hardly ensured.

Decreased acceptance of nuclear power

There is an overall decreased acceptance of the nuclear power and no trust in institutions, which provide nuclear related information, because the information providing is limited and lead by market and business interests. Society is less or even not involved in decisions about the nuclear power policy. There is a realism according the ensuring security, thus not all known or anticipated threats are covered as well as not all threats are thought.

4.4 Environment scenarios



Factor-No.	Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
E1	Consumption patterns in European society	E1A | Increased consumption without a change in behavior	E1B | Increased consumption with adapting towards more sustainability	E1C | Stagnating consumption without a change in behavior	E1D | Stagnating consumption with adapting towards more sustainability
E2	Environmental awareness and education in society in the EU	E2A | No focus on environmental education, less environmental awareness	E2B | Raised awareness, but no own responsibility or action	E2C | Higher environmental education with responsibility for environmental problems	
E3	Agricultural policy in the EU	E3A | Effects of the CAP reform insufficient	E3B | Reformed CAP spreads its positive effects	E3C | New Common Food and Agriculture Policy with food sovereignty	
E4	Development of technology and ecological / environmental sciences	E4A | Chemical and nutrient pollution for more efficiency	E4B | Innovations in food production	E4C | Efficiency and sustainability of novel agricultural systems	
E5	Trade-off between economy and environment in the EU	E5A | Relationship economy vs. environment got worse	E5B | Higher significance of nature-compatible economies	E5C | Trade-off changes slightly in favour of the environment	
E6	Handling the changes in ecosystems in the EU	E6A | Less interventions for ecosystem protection	E6B | Measures for ecosystem protection at local level	E6C | EU measures for ecosystem protection implemented	
E7	Handling the extreme meteorological events in the EU	E7A | Slow adjustment to increased extreme weather conditions	E7B | Adjustment to increased extreme weather conditions		
E8	European forest area	E8A | Further forest degradation	E8B | Stagnating forest degradation	E8C | Forest conversion to sustainable nature orientated forestry	
E9	Agriculture land in the EU	E9A | Exacerbated soil degradation due to the agricultural production	E9B | Use of land for agriculture is still most important	E9C | Effective use of land is getting more important	
E10	Water supply and regulation in the EU	E10A | Increased problems of water scarcity, national regulations	E10B | No lack of water supply, national (municipal) water supply	E10C | No lack of water supply, European regulation	
E11	Urbanization and land use planning in the EU	E11A | Urban sprawl in conflict with agriculture land	E11B | Local and national regulations to meet the rural-urban conflicts	E11C | European regulations for integrated rural-urban development	
E12	Biodiversity importance in the EU	E12A | Measures for biodiversity protection not implemented	E12B | Biodiversity protection: Bio-diversity as important as bio-quantity		
E13	Fishery policy in the EU	E13A | Increased bycatch - No reform of the CFP	E13B | Partial recovery - Reformed CFP with positive effects	E13C | End of overfishing - Reformed CFP with positive effects	

Figure 31: Four bundles of future projections marked by the coloured lines - basis for environment scenarios

4.4.1 “Compliance with green” (green path)

In the green context scenario, big efforts are made towards more resilience and there is an absence of great power conflicts on the global level. The EU is competitive and on the global level there is also a long-term economic stability. There is a strong industrial capability and knowledge base in the security field in Europe. A main focus of the EU is to achieve a worldwide leading position in R&D as well as in security industry. Due to the declining need for security, the risk awareness of the society is sinking. Technology acceptance also differs, depending on its characteristics like suitability for daily use etc. Traditional and social values still remain important in the European countries. Topics like active ageing, life-long education, demographic change and new living models play a significant role.

High responsibility for environment in society

There is a higher environmental education (like awareness of the values of biodiversity) and responsibility for environmental problems. The EU strategy for sustainable development is implemented and providing information to society about environmental aspects based on a partnership approach. Consumption patterns changed towards more sustainability, like healthy eating patterns, moving towards plant-based diets and towards a reduced consumption of meat. There is also awareness of local or global consumption. Economic accounting using indicators regarding economic development as well as environmental sustainability helps to create nature-compatible economies.

Measures for environment protection and reforms at EU-level

There are measures at the European level for better protection and restoration of ecosystems and the services they provide (with influence on prices and markets, property rights, technology development or the local climate). Effective and urgent actions are taken to halt the loss of biodiversity, in accordance with the Convention on Biological Diversity CBD. The “old” CAP is replaced by the New Common Food and Agriculture Policy, which led to changes in international trade in agricultural products according to principles of equity, social justice and ecological sustainability. The global initiatives, i.e. from the World Wide Fund For Nature WWF to stop deforestation reached the goal of conservation, however wood is still an important raw material for production. A reform of the Common Fisheries Policy CFP resulted in recovery of the endangered fish stocks. The realisation that there is no local problem of overfishing but an international one was very important.

Spatial planning and land use concepts compatible to environment

Overarching land use concepts were developed, including food production, conservation of traditional landscapes, biodiversity “production” as well as creating new jobs in rural areas. The spatial planning improves local consumption patterns. Some important improvements of spatial planning were made, like local and national regulations to meet the rural-urban conflicts - Slightly implementation of measurements to reduce urban sprawl due to the changes in national spatial planning laws or reuse of waste urban land or empty buildings.

Focus on sustainability in science and R&D

There is a sustainable scientific focus on the dynamic interactions between nature and society in agricultural systems resulting in innovations of agricultural products, using new technologies (bio- and nano-technology) and improvement of agro ecological engineering: biological pest control, beetle banks, organic farming. Improved weather forecast as well as new architecture and urban planning help to meet the challenges of increasing extreme weather conditions like flooding, hot, dry summers and seasonal water shortages. In general there is no lack of water supply.

4.4.2 “Regulating sustainability” (orange path)

The global situation in this context scenario is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive. In the European countries the ‘western’ value system remains important, but there is a strong focus on securitisation of life, pushed forward by the extensive Security Policy of the EU and a fragmented, yet strong security economy and industry. Despite the high technology penetration of everyday life, people trust in technological solutions. For higher security level citizens even reduce the claims to their fundamental rights and for high security standards public acceptance is given. Technology is generally seen as a solution for security challenges, new technologies are hyped and research is hardly scrutinized.

Regulations at EU level in favour of the environment

Reformed CAP spreads its positive effects due to i.e. solid financial management and controllability or improved definition, who is an active farmer. There is also partial recovery of the endangered fish stocks due to a reform of the Common Fisheries Policy CFP. Agroforestry is supported by the European Agricultural Fund. Transfer payments are made by the EU to support the reforestation. Due to a European law to international tender for the water supply the local water supply was denationalized. This promotes competition within the EU to guarantee the water supply in Europe. There are European regulations also for spatial planning and integrated rural-urban development as well as land use change. Models for rural-urban regions and improved regulation for management of larger projects are developed.

Measures for environment protection at EU-level

The regulations are a base for measures at the European level for better protection and restoration of ecosystems and the services they provide. This includes e.g. an influence on prices and markets, property rights, technology development or the local climate. The urgent actions are taken at the EU level to halt the loss of biodiversity, like the Convention on Biological Diversity CBD or EU strategy for Sustainable Development, were effective. However the adjustment to increased extreme weather conditions is slower: There are partially no lessons learned or there were mistaken investment (also allocation of the EU funds) made after previous events leading to further harm in extreme weather situations.

Higher environmental awareness and education

There is in general higher environmental education (like awareness of the values of biodiversity) and responsibility for environmental problems (partnership approach of Information providing). Consumption shifts gradually to a more sustainable direction, e.g. healthy and targeted nutrition is more and more important, however consumption of agricultural products increased in total as well as the worldwide electricity demand. This leads to a further converting of grassland and forestland to agriculture, thus agricultural production for food consumption is still one of the predominant land-use activities in the EU.

Higher importance of nature-compatible economies

Nature-compatible economies are of higher significance, thus the economic accounting uses indicators based on economic development as well as environmental sustainability. To support the food security innovations in food production were developed, e.g. modern crop varieties; biotechnologies in the production of feedstock for industry or biotechnology applications such as seeds or bio pesticides. The urban zones are used for new forms of sustainable food production (e.g. urban gardening, bringing together small-scale producers).

4.4.3 "Awareness without action" (pink path)

The pink context scenario is characterized by instability on the global level. The framework instability affects as well the economic side, as on the political side of tensions between regions and competing political systems. Also, there is a competition for resources. At the same time, new global players are evolving, asserting their market interests. There is a strong security industry by a fragmented market. The European security industry produces customized security solutions for society. There is a high technology penetration of everyday life (market interests) but also trust in technological solutions. For higher security levels people tend to reduce their rights. Resulting from the economical situation, the society attaches more importance to material interests than to traditional and social values. The social gap grows further.

Gradually responsibility of companies for environment problems

To support the food security the strong industry developed innovations in food production, e.g. modern crop varieties; biotechnologies in the production of feedstock for industry or biotechnological applications such as seeds or bio pesticides. There is a gradually awareness of corporate social responsibility among investors and companies about the real costs of nature degradation. The environmental degradation is not just an externality anymore.

Slightly increased environmental awareness in society

Increased awareness of linkage between consumption and environmental problems happens gradually, but economic aspects are still more important than sustainability, however consumption of agricultural products stagnates. People become more sensitive towards environment, but the environmental education is still not keeping pace with environmental degradation. More information about environmental aspects is provided to society, mostly by the industry.

Less implementation of the EU strategies for environment protection

The implementation of the EU strategies for biodiversity preservation is insufficient, resulting from poor management, inadequate monitoring and enforcement as well as lack of funds. The past trend of landings are continued, thus there were no reforms of the Common Fisheries Policy CFP. Fishing communities suffer, along with fishing jobs and businesses linked to the sector, as fish stocks continue to decline. Also CAP doesn´t meet the environmental and social challenges: There is still a lack of regulation of markets and production (global, cheap production instead of regional high quality production) and therefore more pressure due to yield and harvest. The unsustainable logging and fuel wood harvesting as well as conversion of forests for other land uses like roads and other infrastructure result in further forest degradation.

Solution of the environmental challenges at local or regional level

Grassland and forestland is further converted to agriculture, thus agricultural production for food consumption is still one of the predominant land-use activities in the EU. There are also still conflicts in urban-rural land use, however local and national regulations try to meet the rural-urban conflicts by slightly implementation of measurements to reduce urban sprawl, like reusing of waste urban land or empty buildings. Measures for ecosystem protection are also placed at the local or regional level. There is a national (municipal) water supply system. The adjustment to increased extreme weather conditions is slow: The often mistaken allocation of the EU funds after previous events leads to further harm in extreme weather situations.

4.4.4 “Neither awareness nor action” (yellow path)

The worldwide situation in the yellow context scenario is marked by many conflicts. The global political and economic situation is instable and the EU also loses its power. Global powers and balances shift to few regions and there are conflicts over markets. The long-term financial crisis is not overcome. The market is determined by multinational companies and big players which concentrate on markets with few risks. Still US companies dominate the security market. The social gap grows further and there is a strict differentiation between social classes. As an effect of these developments extreme groups become stronger and are difficult to control. The society is aware that not all risks may be covered by security solutions. Technology acceptance is decreasing in general, more effective research is required.

No change in behaviour towards more sustainability

Consumption, e.g. demand for livestock products, increased without a change in behaviour towards more sustainability. Food consumption patterns significantly impact water requirements. The problems of water scarcity and drought increased, what clearly indicate the need for a more sustainable approach to water resource management across Europe. There is no focus on environmental education. Information providing, concerning e.g. effects of chemicals, pesticides or risks from biodiversity loss, is limited and market driven.

Environmental degradation is still an externality

Chemical and nutrient pollution are still used for more efficiency, thus the development of sustainable technologies is insufficient and there is a lack of innovation in food production. The relationship economy vs. environment got worse: There is no measurement of environmental loss and environmental degradation is still largely treated as an externality.

Land uses in conflict

CAP doesn´t meet the environmental and social challenges, thus there is still lack of regulation of markets and production (global, cheap production instead of regional high quality production), which leads to more pressure due to yield and harvest. Land use pattern determines the value of economic returns from agriculture and forestry production. The intensification of agrarian land and using the land in the most efficient way results in leaching of soils. The unsustainable logging and fuel wood harvesting result in further forest degradation. In general urban sprawl is in conflict with agriculture or forest land: Building on agriculture land and conversion of forests for other land uses like roads and other infrastructure.

No strategies for environment protection

There are less interventions that enhance positive and minimize negative impacts of the degradation of ecosystem services as well as there is still less understanding how dramatic the changes in ecosystems are going to affect us. The EU strategies for biodiversity preservation were not implemented, because of the poor management, inadequate monitoring and enforcement as well as lack of funds. There were no reforms of the Common Fisheries Policy CFP. The fishing communities suffer, along with fishing jobs and businesses. Moreover there is adjustment to increased extreme weather conditions: Less lessons learned on the one hand and mistaken investment decisions on the other hand.

4.5 List of threats as an input for the workshop

The consolidated list of threats was one of the most important inputs for the scenario validation workshop. The descriptions of all listed threats are presented in D.4.4.

Cyber infrastructure	• Governmental cyber espionage and spying • Economic cyber espionage • Cyber warfare • Data leak, - loss, and - trading events - black markets for information • Unexpected results from large scale data fusion • Insider attacks • Cyber extortion (economical) • Governmental sabotage • Terroristic sabotage (Government and critical infrastructure) • Commercial disinformation • Political disinformation • Digital vigilantism • Cyber bullying / reputational damage • Network breakdown – accidental • Network breakdown – natural • Thievery - burglary
Nuclear	• Nuclear power plant accident • Nuclear tests • Nuclear decommissioning • Nuclear material – transportation • Theft of nuclear material/international organized crime and illegal trafficking • Uranium mining • Nuclear espionage • Terroristic CBRN attack • Nuclear waste storage • Nuclear warfare

Environment	• Air pollution • Water pollution • Biodiversity loss • Complex nexus among resources scarcity: food, water, energy & minerals • Deterioration or loss of ecosystem services • Crime – food fraud and food terrorism • Plastic garbage patches as threat for food safety and security • Greenhouse effect/ Global warming • Growing western dependency on oil, gas and import of minerals and high tech metals • Habitat loss and degradation – forest and coral reefs as an example • Introduction of invasive alien species • Loss of arable land • "Natech" disasters (Natural disasters in combination with man-made accidents) • Pharmaceutical residues from pharmaceutical discharges or residues of veterinary drugs • Resource access triggered conflicts within and between states

Table 8: Consolidated list of threats based on all tasks