D4.4 Catalogue of Threat Scenarios

Deliverable submitted in September, 2013 (M21) in fulfilment of the requirements of the FP7 project, 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:	Complete narrative threat scenarios produced through the scenario development of Task 4.4
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
Antje Bierwisch, Fraunhofer ISI
Sonja Grigoleit, Fraunhofer INT
Joachim Klerx, Austrian Institute of Technology AIT

CONTENT

FIGURES

TABLES

Executive Summary

The overarching aim of the 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 base for identifying future possibilities which are solutions and options related to societal security needs.

The research work in WP4 is divided in 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 (see Figure 1).

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 this report, and societal needs which are one of the content of the validation report D.4.5. The first insights supported also the setting of the thematic focus in each of the three domains as well as deriving the key factors (most important aspects) for the development of the scenarios. This was an important step to prepare scenarios. The interview partners represented conventional security research end-users as well as public and civil society organizations that were able to make statements about societal needs 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 the **information mining** (task 4.2, see D.4.1) was to identify possible future threats on the internet. 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 identifying threats using information mining is presented in this report. The two further parts of this analysis related to the weak signals and wild cards is 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 context and threats scenarios and to identify the societal security needs on this basis. This includes the analysis of already existing future studies within the domains cyber infrastructure, nuclear and environment as a preparatory step as well as conducting focus group workshops to gain the expert opinions about the most relevant aspects in the three domains and their future development (see D.4.3), the consistency workshop to build scenarios drafts and discuss them within the consortium and with end-users (see chapter 3 in this report). The main results of these activities were the identification of threats and trends, which are the basis for the

development of scenarios as well as a deeper understanding of the contexts of threat scenarios. The final activity was the scenario validation workshop to identify societal security needs which are the basis for development of solutions dependent of scenarios (see D.4.5).

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, following the principle of the context scenarios. All scenarios are described in this report (see chapter 3 and 4). 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 *threats 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. lack of safety requirements or insufficient providing information about nuclear risks). An additional analysis of threats with *event character* (e.g. terroristic attack or natural disaster) was conducted (see chapter 5). In order to identify *societal security needs* a further analysis was carried out to investigate what happens when a threat occurs in different scenarios (see D.4.5).

The scenario development was conceived as an iterative process of the exploratory activities described above. This iterative understanding is important for an ideal exploitation of the findings provided by the information mining tool, interviews and focus groups. The steps containing the scenario development as well as the identifying threats are presented in figure 1 below:

- Step 1: Development of context and threat scenarios based on the findings of the focus group workshops: 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: There are three sources for the identification of threats: interviews in task 4.1, information mining in task 4.2 as well as focus groups and future studies analysis in task 4.3.
- Step 3: In order to identify societal security needs a further analysis was carried out to investigate, what happens when a threat occurs in different scenarios.
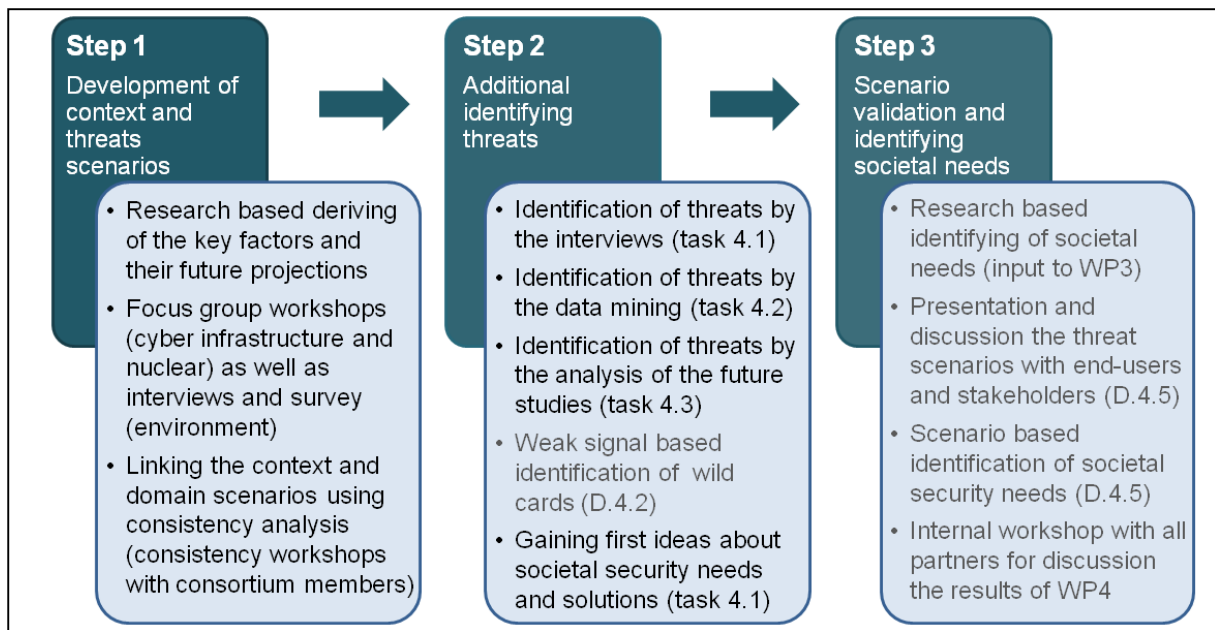
Figure 1: Three-step-process for development of the context based threat scenarios and identifying threats and societal security needs

Legend:
Activities presented in the previous WP4 reports (D.4.1, D.4.3) and this report (black)
Activities presented in upcoming reports D.4.5 and D.4.2 (grey)

The context and threat scenarios describe a wide spectrum of various future possibilities which have different implication on arising societal needs (see D.4.5) and proposing solutions based on different capabilities which could exist or could be missing in these scenarios. The influence analysis conducted for the context scenarios (see chapter 2.2) delivers additional information about which fields (e.g. policy, industry or society) or more concrete which aspects (e.g. security policy, design of security technologies or attitude towards technologies) are the most influent. These are important implications for WP5 which aims at identification of alternative solutions for tackling societal needs, based on different combinations of capabilities and options as well as assessment of portfolios of emerging societal security solutions (composed of capabilities and options, of a technological and institutional nature). Furthermore 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? There are also implications for WP6 which develops rationales for including research topics on a European strategic security research agenda and should integrate stakeholder perspectives in the development process of a set of priorities. For this purpose the representatives of the in scenarios considered fields (e.g. policy, industry, society or R&D) should be involved.

This report presents four different context scenarios, each making different assumptions for the future global powers, economical arrangement, security industry, security understanding and concerns in society, attitude towards security technologies, European R&D infrastructure and other driving forces. Each scenario sets the basis for one chosen threat scenario in each domain: cyber infrastructure, nuclear and environment. The scenarios refer to a period of 10-15 years. For the domain cyber a shorter time horizon has been set (5-10 years, see chapter 3 for the explanation).

The **"Common wealth"** scenario describes an integrated world: 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.

The following threat scenarios and their characteristic based on the **"Common wealth"** scenario:

- **"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.
- **"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.
- **"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.

The scenario **"Fortress Europe"** describes the global situation 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 securitization 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.

The following threat scenarios and their characteristic based on the **"Fortress Europe"** scenario:

- **"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.
- **"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.
- **"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.

As the title suggests the scenario **"Oliver-Twist-Story"** describes world with social inequalities. It 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.

The following threat scenarios and their characteristic based on the **"Oliver-Twist-Story"** scenario:

- **"Going private"**: Industry driven internet governance; Defense driven EU cyber policy; Forced diffusion with growing reluctance; Rising threat level in cyber
- **"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.
- **"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.

The scenario **"Burying heads in the sand"** describes more divided world. 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.

The following threat scenarios and their characteristic based on the **"Burying heads in the sand"** scenario:

- **"Fragmented world"**: Nationalization of internet governance; Non-coordinated cyber policy in the EU; Growing reluctance and slowdown of diffusion; Overall threat level increase.
- **"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.

- **"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.

1   Scenario development approach and identifying threats

Traditionally scenarios are built for two reasons: exploration and decision support. Scenarios explore the future and identify several future perspectives, thus provide a background of decision making (Schomaker 1995, p. 25). Considering a range of possible futures, decision makers will be better informed and their decisions based on this knowledge will be more grounded. 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 if an event occurs, but a tool helping to manage the situation when it really happens. Therefore scenarios within ETTIS describe alternative developments as framework conditions for occurring future threats (WP4) and their handling (WP5).

Thus the scenario methods have been increasingly applied to different questions, many methods have been developed over the years to systematically develop scenarios, which differ from each other mainly in their own specific definition of the individual steps (Geschka/ Reibnitz 1981) or phases (Gausemeier et al. 1996; Godet 2000, p. 10-13), as well as the depth of their treatment. Specific tasks are assigned to the respective steps so that the problem defined at the beginning can be dealt with systematically. A comprehensive overview of the different scenario approaches is given by Kosow, Gaßner (2008, p. 18-19), Herzhof (2005, p. 19-29), Postma, Liebl (2005, p. 162-166) and Götze (1993, p. 71-141). However there are mostly based three main steps:

- Identification and selection of the influencing factors, called key factors in this report;
- Development of future assumptions for selected factors, called future projection in this report;
- Building different and consistent scenarios.

The scenario process conducted in ETTIS contained these three steps; moreover it 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 conducted in the different tasks in WP4, which varies in its comprehensiveness, the first important sub-step is to develop the future assumptions. 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 (Seidl/ Werle 2011, p. 292), for which the necessary sequence of steps or a roadmap are not yet known. Developing assumptions about the future (future projections) is combined with creativity methods in order to ensure that the assumptions do not simply reflect a continuation of past trends. Therefore external experts were involved in the process in order to promote the expansion of perception (see D.4.3 and D.4.5).

The objectives of the scenario development process (Step 1) are listed in the figure below (see figure 2). These objectives were embedded in each focus group workshop as well as the survey.

(1) **Extend the perception**: thinking beyond established pathways
- Future study analysis in the considered field
- Expert identification and selection
- Identification and discussion of the relevant factors

(2) **Handling complexity**: discuss the key factors separately
- Factor evaluation
- Factor selection for the further discussion

(3) **Future alternatives**: Considering alternative developments for each key factor
- Identification of uncertainties
- Development of the future projections

(4) **Bundling of possible developments**: building of different scenarios with a high internal consistency and high external diversity
- Consistency check between the future projections
- Bundling the future projection to scenarios
- Scenario writing

Figure 2: Objectives of the scenario development process
Illustrator: Heyko Stöber

The relevant aspects in context and threat scenarios are described using so called *key factors*. The key factors shape the future of the context, like security in generally, as well as the particular domain. The *key factors in 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 *key factors in threats 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). The possible future developments of the key factors are described in the *future projections*. In the focus group workshops (see D4.3) experts discussed whether only one possible future assumption should be made or whether there are conceivable alternatives. Alternative assumptions were developed for all key factors. The key factors themselves are all considered within the scenarios by the different projections; in turn, the diverse future projections of the key factors are needed for building scenarios which differ from each other. Future projections were identified for contextual as well as for threat related key factors. For example, two possible developments might be assumed for the key factor "Overall development of the EU" (see figure 3, Behlau et al. 2010) at the context level:

- "EU of Institutions": The integration of the European Union was already stagnating in 2013. During the economic and financial crisis, the member states principally looked for individual solutions rather than pursuing a joint European strategy. This trend is

still continuing: the member states focus their attention primarily on optimizing their own economies and joint efforts are limited to security and foreign policy at most.

- "EU of Citizens": The integration of the European Union is largely complete. Europe is now competitive with other regions due to a jointly agreed and closely coordinated economic policy, joint security interests and a unified position in other areas. The political integration resembles the societal integration. The population feels a connection to Europe due to the emergence of an integrated European economic and employment area.
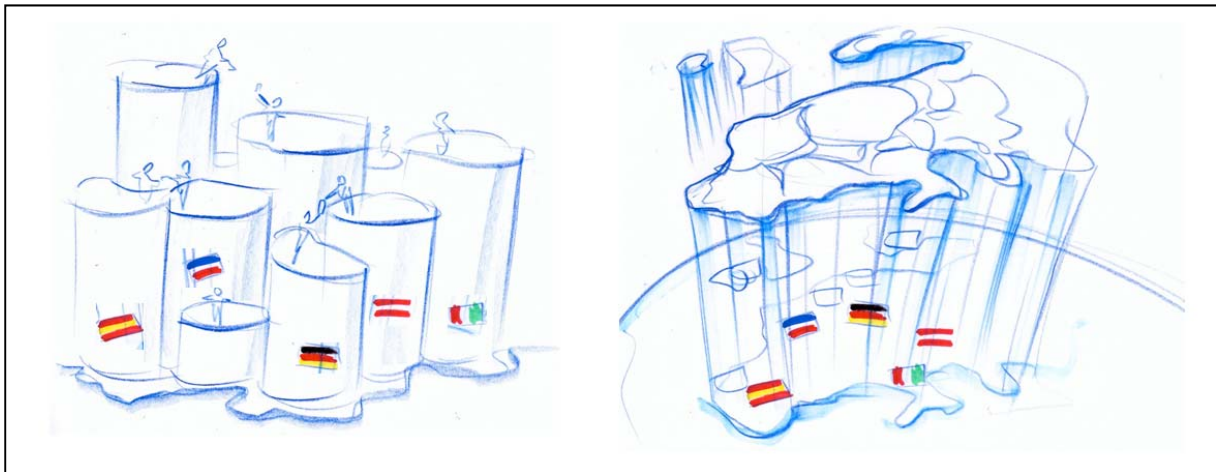
Figure 3: Separation of the member states vs. EU integration and unification as an example for a key factor and its future development
Illustrator: Heyko Stöber

Four consistent **context scenarios** were developed by combining the future projections in a plausible way to so called projection bundles (first level of scenario development, see chapter 3 and figure 4). The most important criteria are (i) firstly the internal consistency (within the future projections in a scenario), e.g. estimation about whether the projections might occur simultaneously in one scenario (ii) secondly the external diversity (within different scenarios), e.g. selection of these scenarios which describe various future situations. Furthermore based on the context scenarios four **threat scenarios** for each domain cyber infrastructure, nuclear and environment were created using the same approach. The results are four context based threat scenarios for each domain (the second level of scenario development, see chapter 4).

Key Factor	Future Projection A	Future Projection B	Future Projection C
Design and orientation of R&D	**5A | Resilience-driven R&D** • Security research is mostly applied research • Shift of the orientation: not to prevent the risk but accept and propose for it • The share of civil security in R&D is larger than military • EU and national security research and innovation focuses on strengthening resilience of society	**5B | Threat-driven R&D** • Security research is mostly applied research and basic research is insufficient • Dual use of research results (civil & military) • Security research is threat driven technology research Focus on securitisation of life	*context scenario paths*
Capabilities & capacities in R&D	**6A | European human resources are sufficient** • European human resources are sufficient • Operational immigration policy • Attractive jobs are offered • Europe has technological, industrial and scientific competences	**6B | Lack of EU-talents & recruitment outside Europe** • European human resources are not sufficient • International recruitment is successful, attractive jobs in Europe • General shortage of well educated, talented young people	**6C | Lack of EU-talents & international recruitment failed** • European human resources are not sufficient, lack of talents • International recruitment has failed • Specialization and focusing on core research fields takes place • Research activities are shifted to institutes outside Europe

green   orange   pink   yellow

Key Factor	Future Projection A	Future Projection B	Future Projection C
Nuclear energy policies in the EU	**N1A | Common nuclear energy policy of the EU** • High interaction between nuclear energy policy, security policy and other policy areas, like environmental policy or fiscal and financial policies. The nuclear energy policy is also linked to other important issues for the EU: climate change; regeneration; world toxic waste exports • Harmonized energy strategy	**N1B | National focus of nuclear energy policies** • Interaction between security policy and other policy areas on EU-level is limited • No framework or agreed strategic approach as well as real long term strategic thinking (100y+) • Tendencies to harmonize the energy strategy are given up; strong influence of lobbies	*nuclear scenario paths*
Share of nuclear energy in the EU member states	**N2A | Increased nuclear energy French way (pro)** • 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 • Economic viability of nuclear power is given • Mechanisms for encouraging nuclear power (on the European level or national	**N2B | Stagnation of nuclear energy Situation like today** • 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 • Nuclear power addresses security of supply only in some countries • Only the member states have programs in favor of the nuclear power and sufficient mechanisms for encouraging nuclear power	**N2C | Decline of nuclear energy German way (anti)** • No assistance programs (on the European level or national level) • Significant investments in improvement of the power plants were not made, while the existing reactors are going to retire (high cost of shutting down) • No assistance programs (on the European level or national level)

green   orange   pink   yellow

Figure 4: Exemplary four scenario paths within the domain nuclear based on four context scenarios

The marked lines in table 1 shows an excerpt of projection bundles which are the basis for the formulation of context based threat scenarios. For example the orange scenario based i.e. on following future projections: threat driven R&D of security technologies as well as sufficient human resources in security research.

These different bundles of the future projections were formulated to short scenario stories (1-2 pages) for the context scenarios as well as for the threat scenarios (see chapter 3 and 4) by describing the future developments in an imaginative way. Scenarios should tell a story which is remarkable, convincing, logical and plausible. They have a descriptive title that transmits the essence of the events described in the scenario. In the following chapters presented

scenarios describe how events might unfold between now and the future in order to capture the dynamics of developments.
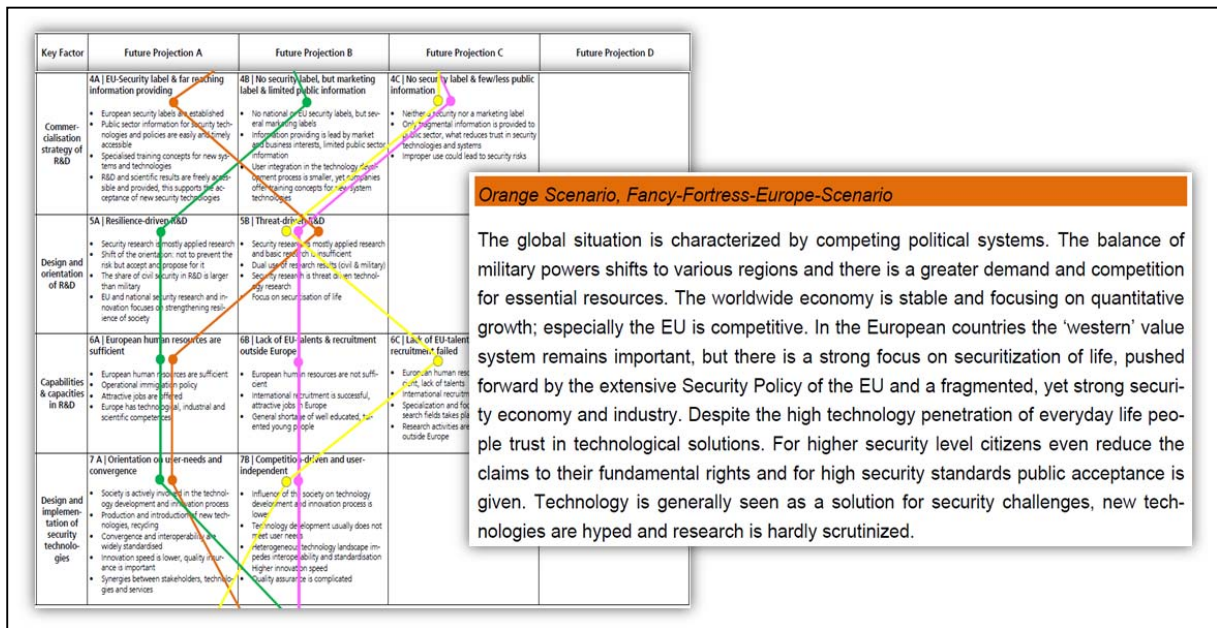
Figure 5: Formulation scenario stories based on the scenario paths

Thus the scenarios include threats with mostly procedural character (e.g. lack of safety requirements or insufficient providing information about nuclear risks), and additional analysis of threats with event character was conducted (e.g. terroristic attack or natural disaster) (see figure 6 and chapter 5). In order to identify **societal security needs** a further analysis was carried out to investigate what happens when a threat occurs in different scenarios (see D.4.5).

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 6: Identifying threats for cyber infrastructure, nuclear and environment – an example

2   Context Scenarios

As mentioned in the previous chapter, building context scenarios contains different steps of research. Chapter 2 focuses on the key factors (2.1), the influence analysis of key factors and the findings of the scenario discussions (2.2) and finally, the four scenarios of the global security environment which are described in short stories (2.3).

2.1 Key factors for context scenarios

For creating context scenarios different key factors are needed, which represent a range of influential global topics. First, a desk research was set up to identify global factors and future projections by analyzing future studies (see chapter 4.3 and D.4.3). At the same time, key factors for cyber infrastructure, nuclear and environment were collected. The next step was to reduce the long list of context key factors to those factors which have a high impact for the ETTIS context. This was performed during the two focus group workshops (see D.4.3), where the participants were asked to comment and prioritize the submitted key factors. In terms of developing the context scenarios there were also synergetic effects with the EU project ETCETERA, as mentioned in the proposal. The following activities were performed in each project:

- Prioritizing the context key factors: The focus group workshops on cyber infrastructure and nuclear within ETTIS (with regard to the relevance for the domains) as well as a scenario workshop with experts from security environment within ETCETERA (with regard to the relevance for security);
- Developing future projections: The expert scenario workshop within ETCETERA as a basis for the future study analysis conducted in both projects;
- Building scenarios: Consistency analysis conducted by the members of the both projects;
- Influence analysis to identify driving forces and scenario discussion: The consistency workshop within ETTIS.

Based on these results a list of 17 global security related key factors was compiled for the context scenarios and the future projections for global key factors were gained. For each key factor two to four future projections were identified which differ from each other.

The following list shows short descriptions of the 17 selected key factors. For the full list of key factors and future projections, see the list in the appendix.

Factor-No.	Key Factor Description
1	**EU-security policy and legal framework** Within this point, general arrangements concerning the EU-security policy and legal framework as well as the harmonization level were discussed. There is a varying emphasize on human or national security. The interaction between security policy and other policy areas differs as well as the international collaboration on terrorism, crime and cross-border conflicts.
2	**General development of EU** The general development of EU-policy includes factors such as appearance of the EU in global affairs and general political influence, enlargement (territory or monetary union) and stability, harmonization level and the efforts for a constitution. Also the solidarity of the citizens with the EU varies (EU citizenship or not)
3	**EU R&D infrastructure** EU R&D infrastructure describes financing and funding (EU or national, public or private), several forms of research cooperation (interdisciplinary, multidisciplinary, networking, cross sectoral research, international research) and the governance of research & innovation (control, management, steering, R&D priorities on a EU level; top-down or bottom-up process of determining R&D priorities). Due to the above mentioned points the overlap of research funding varies and also the degree of competition. The funding of security research plays a special role.
4	**Commercialisation strategy of R&D** Within this factor the role of security labels and commercialization strategies of R&D were discussed. Also public information provision, the evolvement of users in technology development, the accessibility of R&D results and training concepts for users are described.
5	**Design and orientation of R&D** The orientation of security research towards basic or applied research, the budgeting of civil and military research and the dual use problematic are described in design and orientation of R&D. Also the drivers of R&D (resilience or threat-driven) and risk acceptance or securitisation are compared.
6	**Capabilities & capacities in R&D** Capabilities and capacities in R&D highly depend on sufficient human resources. Therefore competence management, education and the education system as well as immigration policies and international recruitment were discussed.
7	**Design and implementation of security technologies** Under this point the influence of society on the technology development and innovation process (orientation towards user-needs or competition-driven developments) as well as the general innovation speed and the way new products are introduced into the market were mentioned. Additionally the implementation of quality assurance and standards/interoperability was described.
8	**Security understanding and concerns in society** This factor describes the balance of risk perception and security needs. Also the role of fundamental rights and resilience in society and the penetration of daily life through security technologies are of high importance.
9	**Cultural influences and social change** The meaning of the value system in society and the detailed arrangement (e.g. role of family, religion and demographic change) are of relevance as well as the social gap and the perception of injustices in the world.
10	**Attitude towards technologies in society** Within this factor the attitude towards science and research as well as technology assessment through society/users are discussed. Also the general technology penetration of life and its impact on society are compared. Further points are the role of virtualization and the possible digital divide.
11	**Global economic arrangement** The worldwide economic stability and general economic situation (e.g. recovery or further crises) are described. It is considered how power shifts and power diffusion take place. Also the public budget and competitiveness of the EU is examined as well as the role of globalization and emerging players.
12	**Production and consumption behaviour** Consumption behavior defines the process of individuals or groups acquiring, using and disposing products, services, ideas or experiences. Also production behavior, value creation and the exploitation of natural resources are discussed. Also the awareness of sustainability is an aspect.

13	**Security industry** The situation on the security technology market is described. It varies especially concerning market leadership (e.g. EU as a global leader or dominating global player), the relationship between politics and industry (e.g. strong alliance or nearly no exchange) and the market fragmentation level.
14	**Relevance of security in different sectors** The usage of security technologies in different sectors (demand and supply side) is described. Additional the vulnerability of infrastructures are classified. Within the security economy there are tendencies to total security or alternatively to risk acceptance.
15	**Role of Intellectual Property Rights (IPR)** The regulation of the knowledge flow (e.g. open source or strict protection mechanism) and the role of intellectual property rights are described (e.g. national patents, EU patent). The usage behaviour of patents and the protection status is differing.
16	**Global shifting powers and balances** The balance of power and its global shift are focused. The relation between political systems, the balance of military power, the extent of terrorism and the aspects of possible conflicts are described.
17	**Global emergencies and disasters** Within this factor the framework conditions in case of global emergencies and disasters are analyzed. Points are the responsibilities (e.g. military, global infrastructure), the general approach to disaster management and varying risk and handling of different catastrophes.

Table 1: Key factors for context scenarios

2.2 Influence analysis of the context key factors and scenario discussion

An important step within scenario analysis is the analysis of the interrelationships between the key factors, as it provides findings about which key factors might be the main driving forces in scenarios. This *influence analysis* was carried out during the workshop with the consortium members on 5th and 6th March 2013 in Frankfurt (consistency workshop). The objective was to achieve within the ETTIS consortium a common understanding of (i) how the context factors influence each other and as a consequence (ii) which will be the most crucial interrelations of factors for shaping the different context scenarios.

In the influence analysis each factor was checked to which extent it is influenced by every other factor and vice versa. Another part of the task was also to record in writing the rationales behind the assigned points. A scale of 0 to 3 has been used: 0 = no direct influence, 1 = weak direct influence, 2 = average direct influence and 3 = strong direct influence. Finally, all the points were totalized per factor in the columns "∑ passive" for the level of influence by the other factors and "∑ active" for the level of influence of the factor on the other factors. Table 1 shows a list of the 17 context factors and the sum of active and passive influence points that were allocated during the consistency workshop.

	Factors context	Σ passive	Σ active
1	EU-Security policy and legal framework	27	23
2	General development of EU	23	21
3	EU R&D Infrastructure	25	18
4	Commercialisation strategy of R&D	25	21
5	Design and orientation of R&D	33	22
6	Capabilities & capacities in R&D	28	21
7	Design and implementation of security technologies	36	17
8	Security understanding and concerns in society	24	29
9	Cultural influences and social change	18	28
10	Attitude towards technologies in society	25	31
11	Global economical arrangement	20	36
12	Production and consumption behaviour	23	27
13	Security industry	29	31
14	Relevance of security in different sectors	23	18
15	Role of Intellectual Property Rights (IPR)	18	21
16	Global shifting powers and balances	23	37
17	Global emergencies and disasters	27	26

Table 2: Context factors and their passive and active influence levels

The influence analysis of the context factors leads to several general conclusions in regard of the importance of certain factors for the context scenarios:

- Out of the 17 context factors which are more or less specific and detailed factor 16, "global shifting powers and balances", came out to be the most influencing one, closely followed by factor no. 11, "global economical arrangement". They have a strong impact on politics and the economic arrangement as well as on society and are therefore guiding for designing the context scenarios.

- The factors "security industry" (13) and "attitude towards technologies in society" (10) have the same high influence on other factors. In contrast to the estimated strong influence of the factor "security industry" the factor "design and implementation of security technologies" (7) is the one that is influenced the most by all the other factors. The strongest influencing factors are in this case not only the economy-driven ones but also factors 1, 6, 8 and 10 which are policy-driven respectively society-driven. Accordingly, this may lead to the conclusion that the performance of the security industry itself can be as well influenced by a precise policy-making as by the attitude of the society at an early stage, which is e.g. the design and implementation of security technologies. The same logic applies to the factor "design and orientation of R&D" (5) which is the one with the second-highest influence by every other factor.

- Vice versa, the factor "design and implementation of security technologies" (7) has the lowest impact on other factors, except for "security industry" and for the "attitude technologies in society" (10). The rational for this estimation is that design is mostly oriented on the prevailing circumstances and their implementation serves as a mirror of the latter. Therefore there is a high influence on the attitude of the society.

- Further factors which scarcely influence the others are "EU R&D infrastructure" (3) as it does not affect most of the factors actively and "relevance of security in different sectors" (14) due to its primarily micro-level impact. The factors 3, 4, 5 and 6 which are related to R&D are also ranked lower, especially as they are taken for being rather invisible in society. Nevertheless it is seen that R&D-driven factors are at least at an

average level influenced directly by economics, industry and politics as they can also be actively shaped by them.

- In contrast to all the other factors, which are either strongly influenced by the others or do strongly influence the other factors themselves, the "role of IPR" (15) seems to be of little importance within the influence analysis: It scarcely records influence on other factors ($\sum$ active 21) and is hardly influenced by them ($\sum$ passive 18). The two factors that have a high impact on the role of IPR are the "attitude towards technologies in society" (10) and the "production and consumption behaviour" (12). As a result, for the context scenarios the factor "role of IPR", respectively its projections are primarily linked to the attitude of the society. On the other hand, the participants also came to the conclusion, that the "role of IPR" can have a high impact on the "commercialization strategy of R&D" (4), "design and implementation of security technologies" (7) and also on the "production and consumption behaviour" (12).

This influence analysis delivers information about which fields (e.g. policy, industry or society) or more concrete which aspects (e.g. security policy, design of security technologies or attitude towards technologies) are the most influent. These are important implications for WP5 which aim is to identify alternative portfolios of solutions for tackling societal needs, based on different combinations of capabilities and options as well as assessment of portfolios of emerging societal security solutions (composed of capabilities and options, of a technological and institutional nature).

Besides the influence analysis a further important step within the scenario analysis, a scenario building based on the *consistency analysis*, was carried out. An important step within this process is generating a consistency matrix, where the fields contain consistency values between the influence factors of the future development. The consistency matrix is used for generating bundles of influence factors projections, which are the base for the scenario writing. The internal consistency (within one scenario) is an important attribute of any scenario as well as the external diversity (between different scenarios). Especially by complex problems with a large number of influence factors, the detailed analysis using the consistency matrix is recommended. For each pair of projections of different influence factors, WP4 team estimated, how compatible the two projections are to each other (see figure 7): 5 = strong consistency, 4 = consistency, 3 = no direct relationship, 2 = partial inconsistency and 1 = total inconsistency. This estimation sets a basis of which future projections should or shouldn´t appear in the same scenario.

1 strongly inconsistent 2 inconsistent 3 neutral 4 consistent 5 strongly consistent	1 EU-security policy and legal framework		
	1A | Human orientation of overarching EU security policy	1B | National orientation of EU security policis	1C | Defence-oriented security policies
2A | Strong development of Europe and further integration	5	2	1
2B | EU of different nations and different integration levels	3	4	3
2C | Decreasing importance of EU	2	4	5
2D | European political union with new constitution	5	1	1

Figure 7: Consistency matrix to determine synergies and conflicts between future projections – an extract for two future projections

2.3 Global security scenarios

In the consistency workshop five scenarios were presented, named by the colors blue, green, orange, pink and yellow in order to gather the participants' opinion on the scenarios. The group discussions were oriented towards the following questions:

- Which key factors do influence this scenario the most?
- How could you characterize / title this scenario?

The discussion led to the adjustment of some future projections and helped clarify interdependencies and dynamics within the scenarios. As a result, the answers, opinions and recommendations are implemented when editing the prepared scenario drafts. Taking in regard the workshop recommendations the ***context scenarios*** are finally reduced to four: the green, orange, pink and yellow scenario. These scenarios are described in chapter 2.3.

The following four context scenarios based on the bundles of future projection which are marked by the four different lines in table 2. These different bundles of the future projections were formulated to short scenario stories for the context scenarios (see chapter 2.3.1-2.3.4). Figure 8 shows an overview of the characteristics of each context scenario.
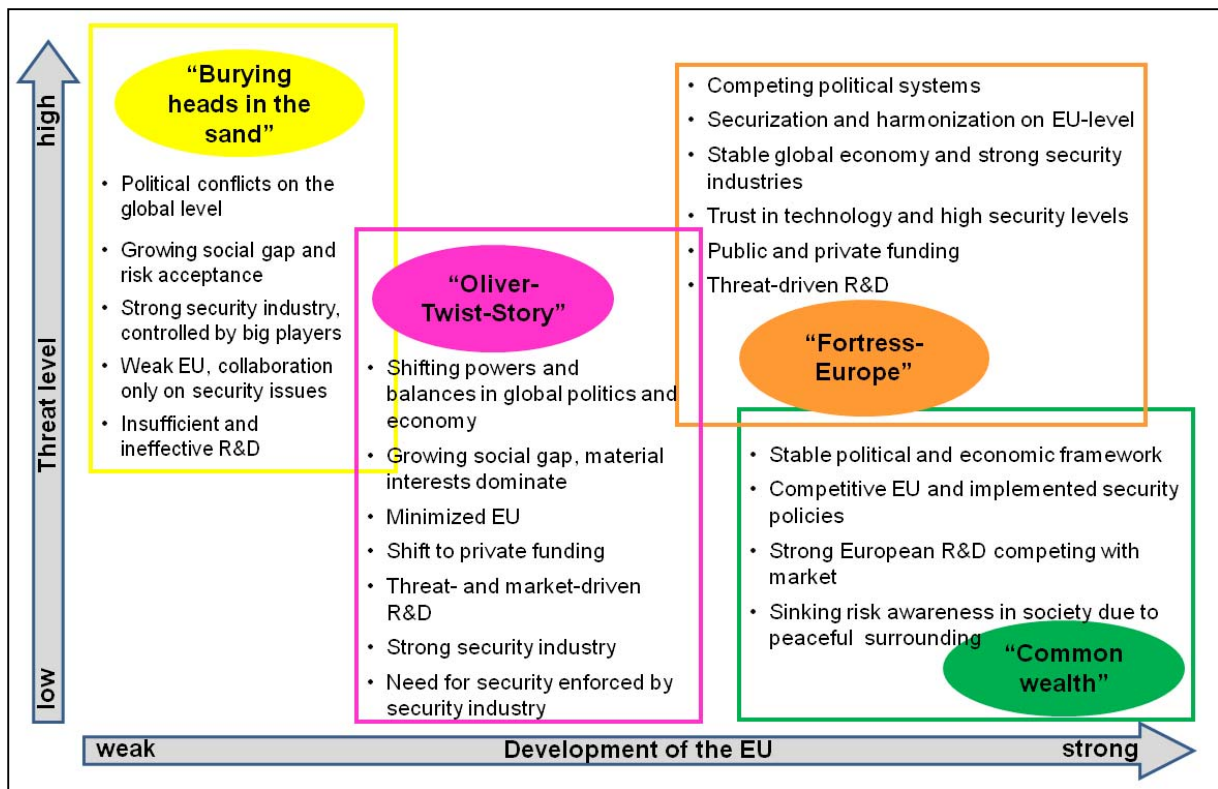
Figure 8: Characteristics of the context scenarios in overview

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 & de-globalization
17	Global emergencies and disasters	17 A | Overwhelming international system	17 B | Interest-driven interventions	17 C | Underinvestment of infrastructure	

Figure 9: Four bundles of future projections marked by the coloured lines - basis for context scenarios

2.3.1 "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.

2.3.2 "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 securitization 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.

Securitization and harmonization on EU-Level

On the EU-level harmonization is far driven, also the enlargement of the EU and the monetary union. An example for harmonization 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 securitization 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.

2.3.3 "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 commercialization 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 harmonization 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 securitization 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 standardization. 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.

2.3.4 "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 standardization 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.

3   Context based threat scenarios

As described in the previous chapter, scenarios were built at two levels, context scenarios (global security scenarios) and threats scenarios (scenarios of cyber infrastructure, nuclear and environment). The process of creating threat scenarios also contained identifying key factors and future projections for each domain (see D.4.3). The main steps in this process were focus group workshops as well as interviews and survey which delivered key input to prioritizing of the key factors and identifying future projections.

We used the consistency workshop to gather participants' opinion on how compatible the developments in each domain (described in different future projections) are with the context scenarios, as threat scenarios should be embedded in different frameworks set by the context. The discussion led to the adjustment of some future projections and helped clarify interdependencies and dynamics within the context threat scenarios. As a result, the answers, opinions and recommendations are implemented when editing the prepared drafts of *context based threat scenarios*, four scenarios (the green, orange, pink and yellow) for each domain.

The context based threat scenarios are presented as follows:

- Scenario bundles and overview of scenarios: (i) Figures 10, 12, 14, 16 show an overview of the characteristics of each context based threat scenario. (ii) The bundles of future projection are marked by the four different paths (see tables 11, 13, 15, 17);
- The different bundles of the future projections formulated to short scenario stories for cyber infrastructure, nuclear and environment;
- Underlying data for scenario building: (i) The key factors of the threat scenarios are presented in figures 19-21 in the appendix as well as the direct interfaces with the context key factors which were useful for linking the context and domain scenarios. (ii) The full list of key factors and future projections is presented in appendix (see tables 11-13).

The scenarios refer usually to a longer period of time ("a jump" of 10 years in time and more). If the horizon is much shorter, scenarios may strongly correspond to the present situation and be just a creative description of the modified status quo. If the time frame is set too far in the future, scenarios may lose their relevance for the implementation in strategic decisions. The considered time horizon differed across the different domains. For the domain cyber a shorter time horizon has been set (5-10 years), opposed to the domains nuclear with a longer time frame (10-15 years). The reason for this is that the cyber domain is characterized by technologies with shorter and dynamic innovation cycles and is therefore subject to a constant change. Nevertheless, the projections for cyber infrastructure as well as those for nuclear may be implemented in the same context scenarios. This is possible due to the fact that the pathways described by the context scenarios consist of general factors and aspects which are valid for faster as well as for slower innovation cycles. Independently and in regard of different timeframes, the experts of the two workshops identified likewise similar context factors to be the most influential.

3.1 Context based threat scenarios of cyber infrastructure

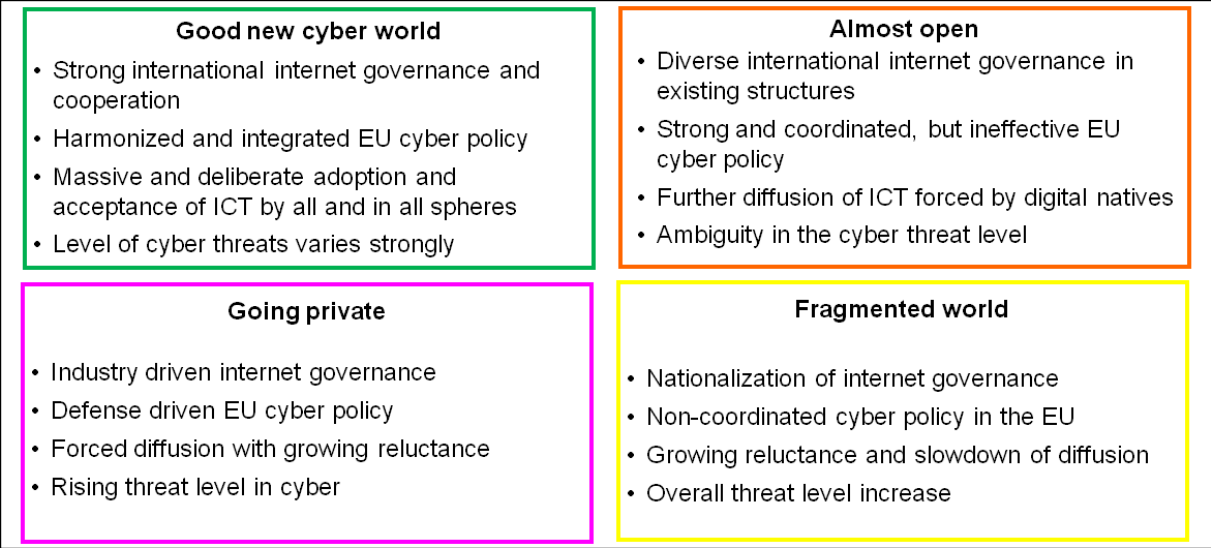| **Good new cyber world**	**Almost open**
• Strong international internet governance and cooperation • Harmonized and integrated EU cyber policy • Massive and deliberate adoption and acceptance of ICT by all and in all spheres • Level of cyber threats varies strongly	• Diverse international internet 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	**Fragmented world**
• Industry driven internet governance • Defense driven EU cyber policy • Forced diffusion with growing reluctance • Rising threat level in cyber	• Nationalization of internet governance • Non-coordinated cyber policy in the EU • Growing reluctance and slowdown of diffusion • Overall threat level increase

Figure 10: Characteristics of the cyber infrastructure scenarios in overview

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

3.1.1 "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 standardization 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.

3.1.2 "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 securitization 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.

3.1.3 "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 organizations 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 nationalization 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.

3.1.4 "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.

Nationalization 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 nationalization*. 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.

3.2 Context based threat scenarios of 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
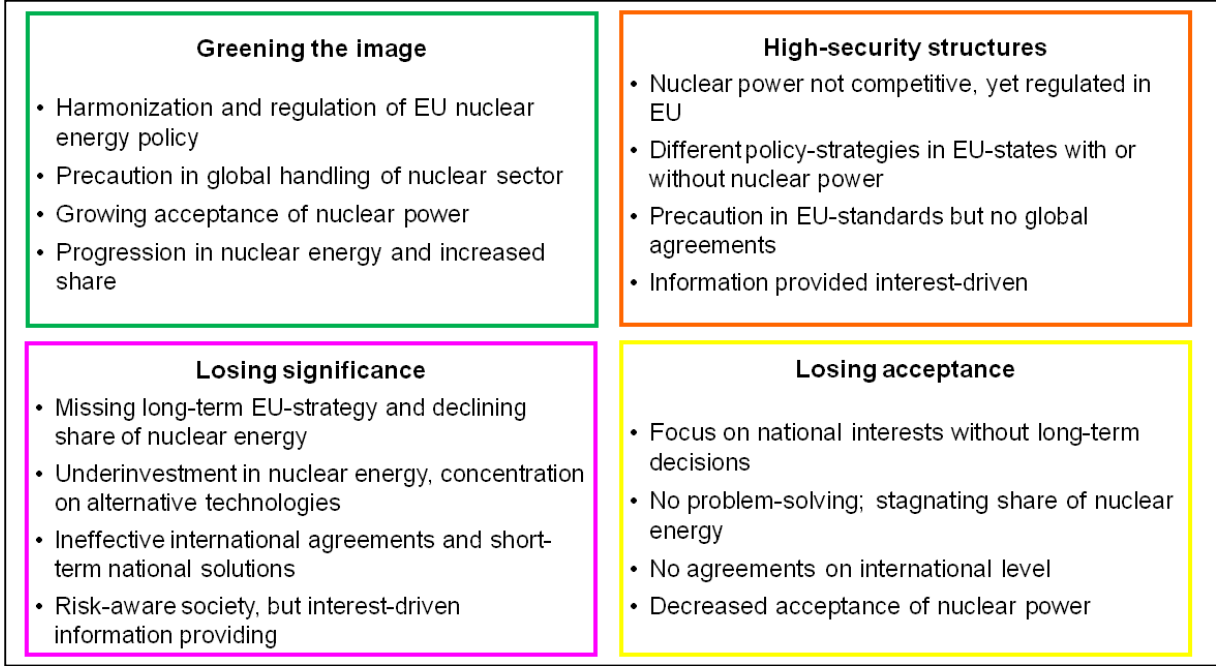- Decreased acceptance of nuclear power

Figure 12: Characteristics of the nuclear scenarios in overview

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

3.2.1 "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.

Harmonization 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 harmonization 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 utilization (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.

3.2.2 "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 securitization 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 harmonization 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 utilization (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 securitization 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.

3.2.3 "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.

3.2.4 "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 utilization (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.

3.3 Environment

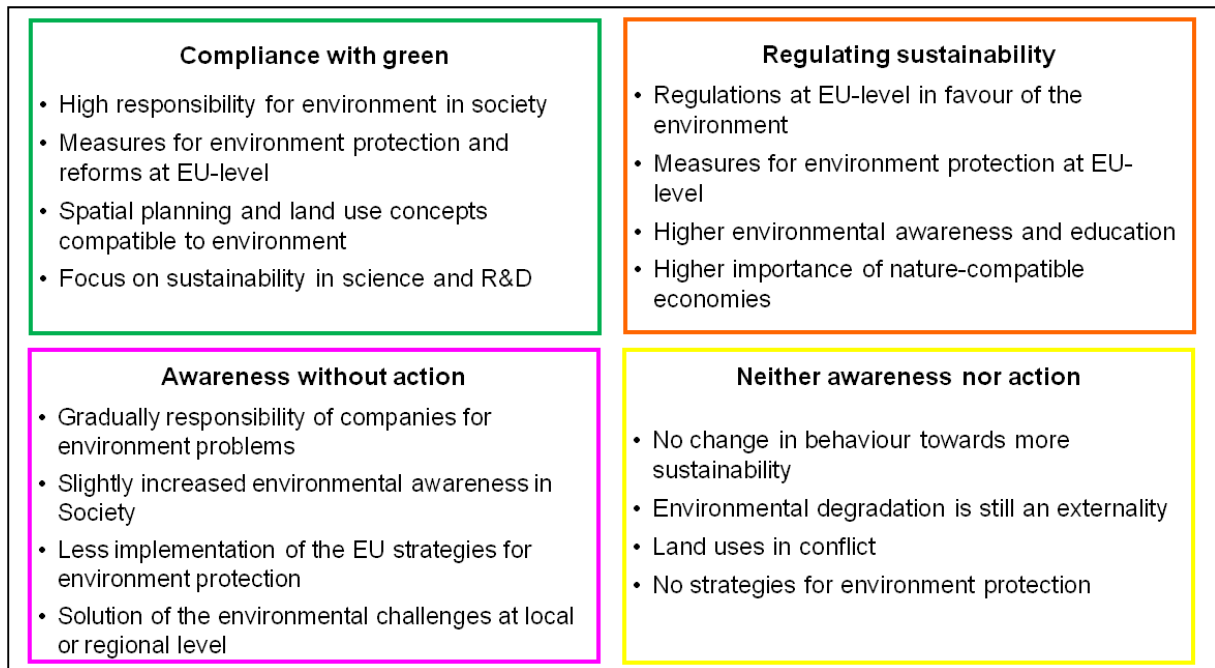| **Compliance with green**	**Regulating sustainability**
• High responsibility for environment in society • Measures for environment protection and reforms at EU-level • Spatial planning and land use concepts compatible to environment • Focus on sustainability in science and R&D	• Regulations at EU-level 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	**Neither awareness nor 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	• No change in behaviour towards more sustainability • Environmental degradation is still an externality • Land uses in conflict • No strategies for environment protection

Figure 14: Characteristics of the environment scenarios in overview

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

3.3.1 "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 realization 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.

3.3.2 "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 securitization 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).

3.3.3 "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.

"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 Identifying threats to society

As the scenarios include threats with mostly process-related character (e.g. lack of safety requirements or insufficient providing information about risks) an additional analysis of threats with event character (e.g. terroristic attack or natural disaster) was conducted. That was the basis for identifying societal security needs in the finale step of WP4 (see D.4.5).

The analysis was generally divided in three 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 "Scenario development and identifying societal needs" by an analysis of future studies, expert discussions in the focus groups (cyber infrastructure and nuclear) as well as interviews and survey (environment). Each task delivered various threats to society. Additionally the task 4.1 delivered the first ideas of societal security needs as well as solutions (see D.4.1 and appendix in this report).

The additional threats mostly have an event character, yet threats with process-related character were also identified in order to complement the threat descriptions in scenarios.

4.1 Interviews with key stakeholders

The main aim of the interviews was to get a detailed picture of threats, needs and security solutions in the three domains cyber infrastructure, nuclear material and environment. Together with the focus group workshops, the interviews provided a good way to include the point of view of experts and end-users complementing our own desktop-research and weak signal scanning.

The first phase of interviews was conducted until January 2013 and was reported in deliverable D4.1. The results of D4.1 were mainly used to set a thematic focus in each of the three domains and also to derive the key factors for the development of the scenarios. The second phase of the interviews was done on the basis of the first scenario drafts and includes the interviews conducted until June 2013. This second phase of interviews was carried out to refine the final picture.

Apart from the interviews, D4.1 also used the deliverables and final reports of previous projects engaged in current and future threats and social needs in order to not duplicate their results. The following projects and forums were found relevant for our research (i.e. they have a similar focus as ETTIS and the project results are still relevant):

- ESRIF - European Security Research and Innovation Forum
- FOCUS - Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles
- FESTOS - Foresight of evolving security threats posed by emerging technologies
- FORESEC – Europe's evolving security: drivers, trends, scenarios
- ENISA – European Network and Information Security Agency - Threat Landscape, Responding to the Evolving Threat Environment

In this deliverable the new interviews of phase 2 will be analysed and complemented with the results of the interviews of phase 1 to get a complete picture of the overall results of the interviews.

We aimed at reaching a balanced mixture both of the categories of organisations as well as of the thematic domain (cyber infrastructure, nuclear material and environment). We added a forth domain "general" – for all interviews from which we got input about nuclear material, cyber infrastructure and/or environmental issues and also about threats and needs on a more general level.

It was rather difficult to find interview partners with a social security background (e.g. public and civil society organisations) who were willing to speak about nuclear or cyber security. Therefore we added a few interview partners from industry and research organisations to get a reasonable number of interviews.

Organisation	Country	Domain	Category
CLUSIT	Italy	cyber	CSO
Dutch Ministry of Economics Affairs	Netherlands	cyber	Government
Nokia	Finland	cyber	Industry
Privacy International	UK	cyber	CSO
secunet	Germany	cyber	Industry
TU Berlin	Germany	cyber	Research
Catholic Church	Germany	environment	CSO
Dutch Ministry of Infrastructure and the Environment	Netherlands	environment	Government
Environmental defense fund	USA	environment	CSO
Federal Agency for Technical Relief	Germany	environment	Government
Federal Office for Civil Protection	Switzerland	environment	Government
Red Cross	Sweden	environment	CSO
Oxfam	Germany	environment	CSO
Red Cross	Germany	environment	CSO
Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU)	Germany	nuclear	Government
Fraunhofer	Germany	nuclear	Research
Institute for Applied Ecology	Germany	nuclear	Research
Institute for Technology Assessment and Systems Analysis	Germany	nuclear	Research
International Physicians for the Prevention of Nuclear War	USA	nuclear	CSO
United Nations Institute for Disarmament Research	Switzerland	nuclear	Government
Crisis Management Initiative	Finland	general	CSO
International Alert	UK	general	CSO
London Fire Brigade	UK	general	Government
Scandinavian Islamic Organisation	Sweden	general	CSO
Swedish Armed Forces	Sweden	general	Government
Swedish Civil Contingency Agency	Sweden	general	CSO
The Finnish National Rescue Association	Finland	general	CSO

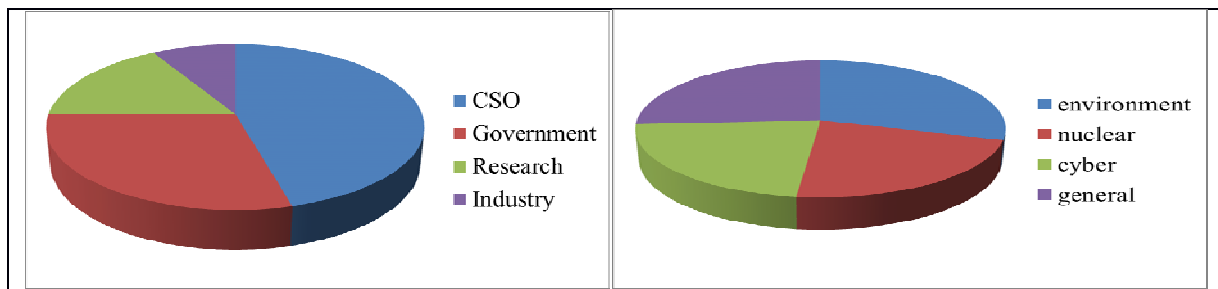Table 3: List of the organisations of the interviewees

Figure 16: Domain and category of the conducted interviews.

To get an impartial picture over threats, needs and security solutions in the three domains we developed an interview guide with rather open questions to make sure that we do not restrict the answers of the stakeholders in any way.

We also took into account the different backgrounds of the interviewees and prepared an introductory letter containing explanations of the aim of the interviews and the used terms, like threat, need and security solution (see Annex 8.2 of D.4.1 Threat Scenarios). The list which contains the questions for experts as well as further basic definitions are presented in D.4.4.

Generally it was observed that the statements of the interviewees gave new insight and new points of view to the systematic of threats described in previous reports. They added urgency to the mentioned threats and gave easy-to-understand examples.

The results of the interviews for each domain are described in detail in the appendix (see chapter 6.3). The list of threats is presented in table 4.

Cyber infrastructure
• Lack of education of the end-user (i.e. end-users do not care about a proper configuration of the systems, like fire-walls, virus-scanner or software updates)
• Vulnerability of commercial systems (systems are often put on the market when they are acceptably solid - there is a lack of built-in security measures and rigorous testing of technologies)
• Backdoors (examples for security risks due to backdoors are the Vodafone phone tapping scandal in Greece or the case of the Chinese telecom firms Huawei and ZTE)
• Attacks on vital utility companies
• Attacks on industrial control systems (SCADA)
• Vulnerabilities in the EC-card and credit card system
• Cyber crime
• Cyber-war
• Lack of trust of consumers (if cyber-crime increases further, this might have the impact that the consumers start to withdraw themselves from the market)
• Security policy introduced in technology (general security responses might increase the risk of security, e.g. identity cards, smart meters)
• Social media (social media present an increasing potential for good but also bad "movements")
• Cyber espionage

Nuclear
- Nuclear warfare   - Nuclear proliferation   - Terrorist attacks with dirty bombs   - Terrorist attack on a nuclear site   - Accidents at nuclear power plants
Environment
- Climate change (impacts: sea-level rise, glaciers melt, crop shortfalls, change of Gulf Stream, spread of tropical disease, loss of biodiversity, new migration flows)   - Hurricanes   - Sturm surge   - Flooding   - Snowdrifts   - Oil spill   - Earthquakes   - Tsunami in the Mediterranean   - Avalanches   - Pandemics   - Impact of natural hazards on critical infrastructure   - Natural resource scarcity (oil, rare earth elements, etc)   - Water scarcity   - Loss of biodiversity   - Genetically modified crops   - Nanotechnology   - Land grabbing   - Biofuels   - Environmental pollution   - Chemical accidents   - Depletion of fish-stock   - Solar storms

Table 4: Interviews with stakeholders – Domain specific threats

4.2 Weak signal mining

The main goal of the weak signal mining activity was to identify possible future threats, based on discussions on internet. However, the interpretation of which signal might be a future threat, depends very much on human interpretation. Therefore, a two step strategy was applied. In a first step, a community was identified; in which members of the community publish content about future threats on the internet. In a 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 to get hints about possible weak signals for future threats.

Based on a dataset of about 160,000 links to sites containing the phrase "future threats", discussion topic where clustered and identified, with regard to their potential for a weak signal. In communication theory a signal is a sign with a specific meaning to the receiver of this signal. If the communication is build up with a carrier signal of white noise, than a signal

with a specific meaning has to be different from the white noise. As a core concept in signal processing, the signal is the peak that transfers the information from the sender to the receiver. Consequently, a weak signal is a signal, which is statistically not very different to the carrier signal.

In text mining, the basic corpus, or more precise, the word frequency matrix of the basic corpus, is used as a kind of white noise for the analytical process. The TIA algorithm identifies weak signals, based on changes in word frequency matrix, which are used as indicator for semantic weak signals. These signals can either indicate a threat or an opportunity. It can give hints to resulting future social needs, or can be a wild card. As the following graphic symbolises, it is a good process in semantic analysis, to check first, whether there is a potential for a threat or opportunity, then check, whether there are hints to social needs in the topic and finally check, whether there is a potential for a wild card. For the semantic analysis additional human research was necessary.
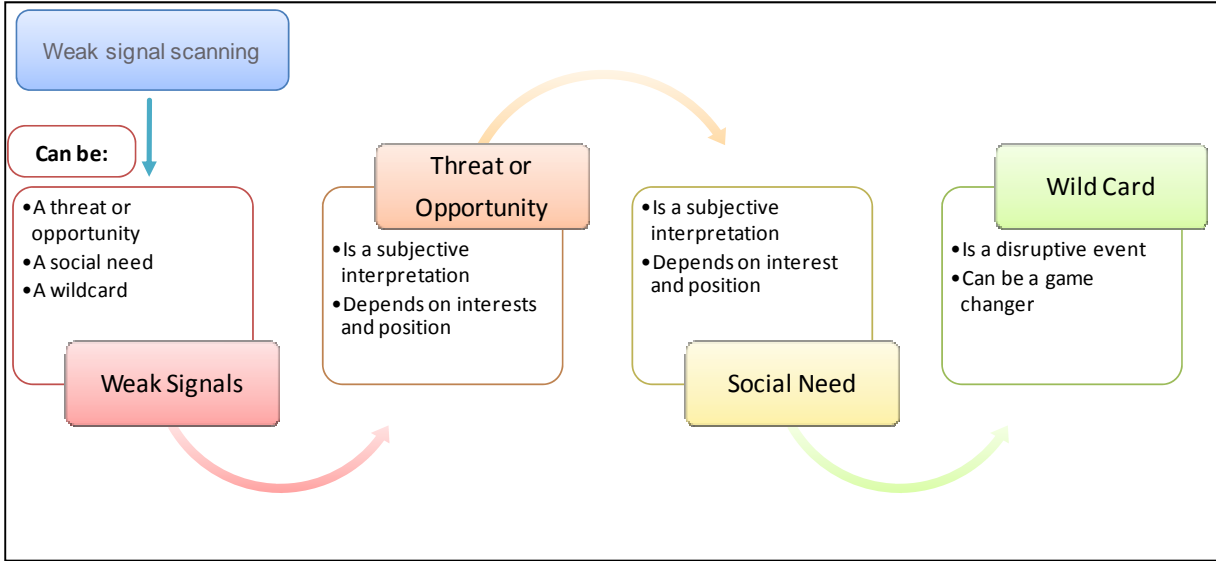

Figure 17: Analytical process in signal mining

The following definitions were used to identify threats, opportunities, social needs and wild cards in the list of weak signals.

Weak signals are small and therefore often early signs to events, which point to future threats, opportunities, needs or wild cards. In particular, the weak signals with a potential to be a wild card often points to future strategic discontinuity. Therefore they have a high analytical value for strategic long term planning.

T**hreats** can be a warning that one is going to hurt or punish someone, they can be a sign of something dangerous or unpleasant which may be, or is, about to happen, or they can be a source of danger.[1] In each meaning, the following three essential elements are part of a threat:

---

[1] http://www.thefreedictionary.com

- a harmful event
- a cause of this event (either accidently or by intention)
- an effect of this event

Based on the wide geographic distribution of threat discussion on the internet, identified by TIA, it became obvious in the analytical work, that a threat is a subjective interpretation of a specific event. If this event is harmful to a person or a group, this event is considered as a threat from all group members. This opinion is not necessary shared by all other humans. In particular, there might be another group, who take advantage from this event. They usually will not consider this event as a threat. Therefore, threats are always subjective expression of a value. The same applies to opportunity. An **opportunity** might either be a favorable or advantageous circumstance, occasion or time, or a chance for progress or advancement. The advantage is usually related to a specific group. Thus this group will consider the favorable event as opportunity.

Wild Cards are high-impact events that seem too incredible to believe in. Therefore they tend to be overlooked in long term strategic planning. Often it leads even to a decrease in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, "wild cards" refer to low-probability, high-impact events, as introduced by John Petersen author of "Out of The Blue - How to Anticipate Big Future Surprises".[2] However more important than probability is, that these topics are not well known and not part of the mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However for strategic long term planning and scenario development they are very important, as they increase the ability in scenario planning, to adapt to surprises arising in turbulent chaotic environments. In trend analysis, they point to trend breaks and tipping points.

Trend as a future oriented concept is misleading. It is a well known fact that it is easy to discover a trend based on historical data on the stock exchange. However it is nearly impossible to learn something about the share price from tomorrow from this. A trend in general is a direction, derived from past data. It is usually based on linear pattern, which only work in a specific context. Trends are usually described by time horizon, impact and geographical coverage. Here in this report, a trend is used to make a distinction between trends and wild cards.

The following table 5 contains list of weak signals which were classified as a threat. A problem arises from the fact, that some threats affect two or more domains. In the following list each threat is listed under each domain which is affected. However in the consolidated list of threats (see table 8) the threat will be listed under the most affected domain.

---

[2] Petersen, J. (2000) 'Out of The Blue - How to Anticipate Big Future Surprises' Madison Books

Cyber infrastructure
• Stuxnet as first SCADA attack software platform
• Advanced persistent threats (APT), like Ghostnet
• Black Market prices explosion of Zero day exploits
• Military cyber attack unites
• Modular botnet development platforms
• Trojan horse software service industry
• Globalisation, strategic sourcing and cloud services
• Global advertising networks and private data exchange
• Dark nets and cryptographic peer to peer nets for anonymous publishing and whistleblowing
• Global black hacker industry and black markets
• Epistemic networks for knowledge exchange in organised crime
• Systemic risk: Takeover of virtual currency supplier, by organised crime
• A new power on the horizon - Global virtual communities
• Living With Terror: Democracy and Terrorism
• A Society of Surveillance?: The National Introduction of ID Cards?
• Defining Paths: The Shape of Islam in the 21st Century
• One Flag, Many Nations: The Establishment of an International Army?
• Will We Have Armies in the Future? Declining Recruitment Rates for the Armed Forces
• Globalisation: Could the Barriers be Going up Again?
• Bio-Breakout: A World Swept by Pandemics
• Saving Lives Through Disaster Prediction
• All the World is a Stage: The Increasing Power of Transnational Corporations
• Serious, Organized and Networked Crime: Criminal Networks in the era of Globalisation
• A Modern Icarus: Could Solar Flares Cause Communication Meltdown?
• Who's Looking at you? Increasing Mass Surveillance
• To Arms: The Growing use of Lethal Force in Violent Crime Across Europe
• Virtually Criminal: the Rise of Internet Crime
• Geoshifts in Innovation
• Sensors and Tracking: Finding Anything, Anywhere, Anytime
• Security: Marrying Technological and Human Approaches
• Understanding Complexity: How to Answer the Big Questions
• A Droid for All Seasons: Robots Become More Versatile
• Surviving Peak Oil
• Dangerous Climate Change and Tipping Points
Nuclear
• Nuclear terrorist attack
• Nuclear espionage of non state actors
• Uncontrolled release of nuclear waste
• Dirty Bombs and CBRN terrorism
• A new power on the horizon - Global virtual communities
• The Shadow of the Bomb: The Risks of WMD Proliferation and Terrorism
• Living With Terror: Democracy and Terrorism
• Defining Paths: The Shape of Islam in the 21st Century
• One Flag, Many Nations: The Establishment of an International Army?

- Will We Have Armies in the Future? Declining Recruitment Rates for the Armed Forces
- Globalisation: Could the Barriers be Going up Again?
- Bio-Breakout: A World Swept by Pandemics
- Saving Lives Through Disaster Prediction
- All the World is a Stage: The Increasing Power of Transnational Corporations
- Inclusive Security?: United Nations Security Council Enlargement?
- Public Service, Private Provider?: Future Implications of the Growth of PFI Schemes
- Serious, Organized and Networked Crime: Criminal Networks in the era of Globalisation
- Raising the Stakes: Will Iran Develop Nuclear Capability?
- A Modern Icarus: Could Solar Flares Cause Communication Meltdown?
- Who's Looking at you? Increasing Mass Surveillance
- To Arms: The Growing use of Lethal Force in Violent Crime Across Europe
- Talking Rubbish: The Struggle to Conquer the Growing Waste Mountain
- Geoshifts in Innovation
- Understanding Complexity: How to Answer the Big Questions
- A Droid for All Seasons: Robots Become More Versatile
- Surviving Peak Oil
- Nuclear NIMBY: Meeting the Challenges of Next-Generation Nuclear Waste Management and Public Acceptability
- Continued Growth in Energy Consumption
- Dangerous Climate Change and Tipping Points

Environment

- Surprising side effects of genetic engineering
- Water pollution and peak water
- Air pollution without boarders
- Land pollution with human waste
- Noise pollution on land and sea
- Light pollution in industrialised countries
- Deforestation, loss of biodiversity and desertification
- Plastic garbage patches in the ocean
- Globalisation of food fraud
- Collapse of space waste
- Acidification of the ocean
- Agro-terrorism
- A new power on the horizon - Global virtual communities
- The Shadow of the Bomb: The Risks of WMD Proliferation and Terrorism
- Eco-Terrorism: A Rising Threat?
- Living With Terror: Democracy and Terrorism
- Defining Paths: The Shape of Islam in the 21st Century
- One Flag, Many Nations: The Establishment of an International Army?
- Will We Have Armies in the Future? Declining Recruitment Rates for the Armed Forces
- Globalisation: Could the Barriers be Going up Again?
- Globalised Migration: Complex Human Transfers
- Return to the Ark
- Bio-Breakout: A World Swept by Pandemics
- Protecting Air Quality: The Effects of Air Pollution in Developed and Developing Countries

- Quenching the Thirst: International Water Shortages?
- All the World is a Stage: The Increasing Power of Transnational Corporations
- Serious, Organized and Networked Crime: Criminal Networks in the era of Globalisation
- A Modern Icarus: Could Solar Flares Cause Communication Meltdown?
- Who's Looking at you? Increasing Mass Surveillance
- Plenty More Fish in the Sea?: The Depletion of Fish Stocks.
- Sowing a Bitter Crop: Global Reductions in Available Arable Land
- To Arms: The Growing use of Lethal Force in Violent Crime Across Europe
- Talking Rubbish: The Struggle to Conquer the Growing Waste Mountain
- The Kraken Awakes: the Impact of a Cataclysmic Seismic Event
- End-game?: A Major Asteroid Impact on Earth
- Gene Out of the Bottle: Could Genes from GMOs Proliferate in Nature?
- The Oil Crisis: Any Light at the End of the Pipeline?
- Geoshifts in Innovation
- Understanding Complexity: How to Answer the Big Questions
- A Droid for All Seasons: Robots Become More Versatile
- Synthetic Chemical Cells – A New Way for the Invention, Discovery, Synthesis and Production of Molecules and Materials
- Surviving Peak Oil
- Continued Growth in Energy Consumption
- Dangerous Climate Change and Tipping Points

Table 5: Weak Signal Mining – Domain specific threats

All weak signals from TIA and in addition the weak signals from sigma scan, which are relevant for security policy, are listed in the appendix (see chapter 6.4). Sigma Scan - is "a searchable repository for horizon scanning papers, designed for government users, ... with 250 short papers "of weak signals"... to challenge assumptions and spark ideas."[3] This list shows the actual ETTIS weak signals and their classification as threat/ opportunity, need or wild card and their classification regarding the main domain. Both classifications are later used to sort the weak signals into their corresponding consolidated list of threats.

In addition to the list of weak signals, with classification, the second table in the chapter 6.4 will give an explanation, why a specific weak signal is considered as wild card. Therefore this list explains in comments, why the weak signal points to a wild card. Weak signals with 9 or 10 should be considered in scenario planning to develop more robust scenarios. Both lists of weak signals are sorted by weak signal. The full list of weak signals, with description will be presented in D.4.2.

4.3 Analysis of future studies and focus group workshops

The stocktaking of the key factors which were relevant for the context as well as for each domain and which should be described in scenarios referred to a broad range of different context related aspects from the following fields which were frequently named: e.g. EU

---

[3] http://www.sigmascan.org/Live/

policy, EU development, socio-cultural developments, trends and drivers in technology, research landscape, ecology and sustainability or economy. However there were also specific research fields for each domain, like sources and types of attacks or attack targets and vulnerability (cyber infrastructure), handling of disposal and transport or material control and accounting procedure (nuclear) and agriculture or forestry (environment).

We analysed almost 300 documents which provided descriptions of different futures related to various aspects from the field of security in general as well as from cyber infrastructure, nuclear and environment. These future studies consider various time horizons. The analysis relies largely on the systematic investigation of secondary sources. These documents represent 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:

- Which are the most important aspects characterising and influencing the field of security today and in the future?
- Which are the most important aspects characterising and influencing the domains cyber infrastructure, nuclear and environment?
- Which are the present and future developments of these aspects?
- Which developments describe various threats?

The first and the second question aim at finding key factors by analysing the aspects described in the future studies. The next step is to capture the situation today and possible future projections of the certain aspect that are given in the literature. For stocktaking of threats the last question was the most important one, thus it delivered the ideas of possible threats within domain.

The results of the future study analysis were the basis for the expert based discussion in focus group workshops (cyber infrastructure and nuclear) as well as interviews and survey (environment). Based on the results of the focus setting within the originally broad defined domains (described in D.4.1) experts of the following fields were invited to attend the focus groups workshops as well as the survey (see D.4.3):

- The focus group workshop on the future of cyber infrastructure security addressed i.e. aspects like cyber attacks and cyber crime, social network and privacy, information risks, data storage, vulnerability of existing and new information technologies (e.g. mobile phones).
- The focus group workshop on the future of nuclear material dealt with aspects like nuclear power plants, use of nuclear material, nuclear accidents, waste management risks and dumping of hazardous waste.
- Interviews and survey for the domain environment primarily focused on the environmental degradation, i.e. biodiversity loss and invasive alien species, water pollution, land use and pollution, deforestation and soil erosion, population growth as well as potential conflicts related to the resource scarcity and resource distribution.

By involving experts, a deeper understanding of the contexts of the scenarios was gained as well as the further input to the identification of threats which is showed in table 6 below.

Cyber infrastructure
- Cyber espionage   - Cyber warfare   - Data loss   - Data leakage   - Insider attacks   - Cyber extortion   - Sabotage   - Identity theft   - Desinformation   - Reputational damage   - System failure network attack Bullying   - Accidental network breakdown   - Distributed Denial of Service attack   - Online fraud   - Man in the middle attack   - Drive by attack zero day exploits   - Social engineering attack   - Online thievery   - Phishing
Nuclear
- Reprocessing waste   - Radionuclide migration   - Nuclear accidents   - Nuclear winter   - Growing energy demand and production   - Gamma radiation and alpha decay   - Proliferation of nuclear material   - Arm race and access to CBRN material   - Uncontrollable use of nuclear material   - Theft of nuclear material   - Transportation of nuclear material
Environment
- Environmental/ Bio-degradation   - Species extinctions   - Species abundance and community structure   - Habitat loss and degradation   - Shifts in the distribution of species and biomes   - Deterioration or loss of ecosystem services   - Nitrogen deposition   - Trends in invasive alien species   - Soil salinity   - Loss of arable land   - Soil erosion CO_2 emissions/ greenhouse effect

- Water and land pollution
- Land use (overuse/ transformation)
- Decreased precipitation
- Increased precipitation
- Acceleration of environmental degradation
- Hydrological changes
- Global warming
- Droughts and floods
- "Natech" disasters
- Water scarcity
- Resource shortages
- Complex nexus among resources scarcity: food, water, energy and minerals
- Growing Western dependency on oil, gas and import of minerals and high tech metals
- Resource and climate change triggered conflicts within and between states
- Chronic diseases, epidemics and pandemics

Context

- Border infringements (sea border/ land border)
- Armed attacks with conventional weapons
- Use of unconventional and self-made weapons
- Conventional crime-related violence
- Social, political, cultural and economic unrests
- Territorial conflicts
- Other conflicts
- International terrorism
- Attacks to large scale, soft targets and public infrastructure
- Nexus to international crime
- War on terror
- Ineffective anti-terrorism measures
- Radicalism
- Changing nature of crime
- International organized crime and illegal trafficking
- Economic crimes
- Poverty, overcrowded, urbanization
- Fragile and weak states
- Weak infrastructure in developing countries
- Major war
- Strong anti-Western theocracy and new regimes
- Global governance failures
- Multi polar world order
- Blocking and failure
- Economic decline
- Lack of maturity and efficiency in EU security market
- Growing globalization and dependency
- Growing number of global players
- Vulnerability of European values
- Growing disparity and marginalization among states

- Growing disparity and marginalization within states
- Financial crises
- Short term economic crises
- Slow economic integration of post-communist economies
- Unmet expectations of new generations
- Air transportation system
- Disruptions to critical infrastructures
- Change of terrorism/ crime
- Dependency on technology
- Technological vulnerability
- Technological overflow
- Risks from new technologies (including ethical)
- Slow pace of technological innovation and adoption lag
- Rapid population growth
- Emergence of mega cities in the South
- Ageing population in the West (Europe and Japan)
- Rapid increase of ethical diversity in the West population
- International migration
- Changing roles of individuals in crisis
- Revised patterns of living

Table 6: Analysis of future studies and focus group workshops – Domain and context specific threats

4.4 Consolidated list of threats

The focus of the further work was on prioritising and discussing the identified threats from each task within the WP4 team and describing of selected threats in detail. This was a necessary step to handle the large number of these threats, structure them and find a common level of threat description. The prioritising was based on the following criteria:

- relevance for the society,
- extent of the impact,
- relevance for security,
- relevance for the EU.

In order to structure the stocktaking of threats we used a template which contains the answers to following questions (see table 7): Which are the relevant threats for cyber, nuclear and environment? Which 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?
Affected areas	In which areas this threat might be relevant? For which institution this threat might be relevant? What kind of influence might this threat have on these areas / institutions? What might be potential risks / opportunities?
Affected regions	For which regions / states might this threat be relevant? What kind of influence might this threat have on these regions? What might be the potential risks / opportunities?
Affected domain	Is this threat relevant for the context situation in general? Which domain might be affected (cyber infrastructure, nuclear, environment)?

Table 7: Template for identifying threats for cyber infrastructure, nuclear and environment

Thus there were large overlaps between the stocktaking results of the different tasks 4.1, 4.2 and 4.3 to 4.4, a consolidated list of threats was developed (see table 8). The descriptions of all listed threats are presented in the appendix.

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 technological 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

5 Summary and outlook of further research

This report describes the two first steps of the scenario development as well as the identifying threats, presented in figure 17 below (step 1 and 2): firstly the approach and secondly the results which are ***context based threats 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, described in D.4.5, contains the following activities (see underlying points in the figure 18 below, step 3):

- 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 (D.4.5).
- 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 (D.4.5).
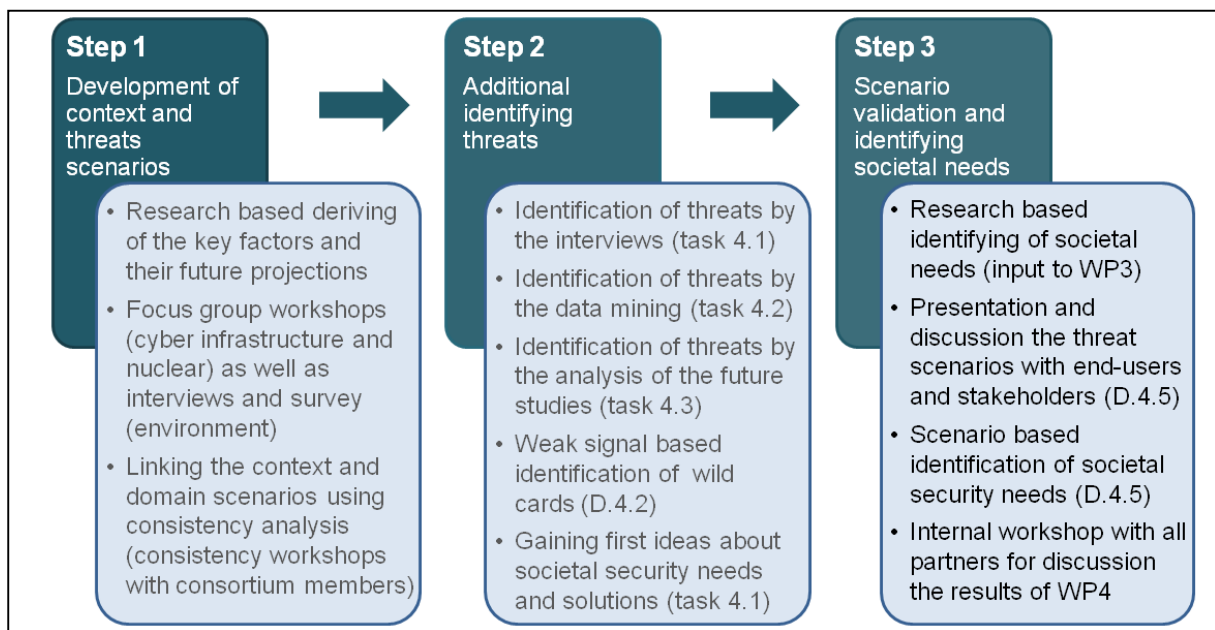

Step 1
Development of context and threats scenarios
- Research based deriving of the key factors and their future projections
- Focus group workshops (cyber infrastructure and nuclear) as well as interviews and survey (environment)
- Linking the context and domain scenarios using consistency analysis (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 18: 3rd step - identifying societal security needs

The scenario validation workshop will deliver input to the final task (4.5) within WP4. In order to validate the outcome of the previous scenario development process this workshop will contribute firstly to the identification, discussion and prioritising of threats for cyber infrastructure, nuclear and environment. Secondly it will provide 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 will be the user group, which encompass most relevant stakeholders from the 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 in this report presented 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. 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.

A 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.
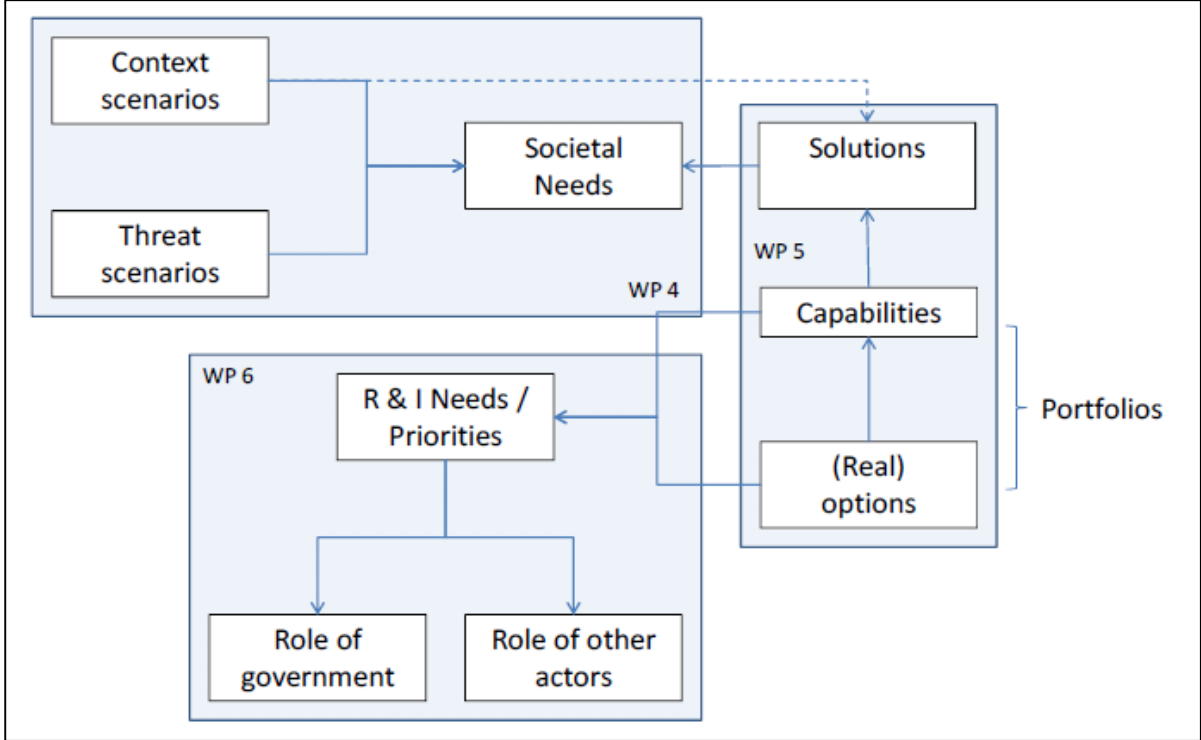

Figure 19: Transfer of the research results from WP4 in WP5 and WP6

6 Appendix

6.1 Basis for scenarios: Key factors and future projections

6.1.1 Context

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** • EU-level: overarching security policy and decision making • More focus on human security than on national security • High interaction between security policy and other policy areas • Fully harmonised alignment of legal framework • Good international collaboration on terrorism, crime and cross-border conflicts	**1B | National orientation of EU-Security-Policy** • Alignment of legal framework is partially harmonised • More focus on national security than on human security • Interaction between security policy and other policies areas is limited • Decreased international collaboration on terrorism, crime, cross-border conflicts and on reducing weapons of mass destruction	**1C | Defence-oriented EU-Security-Policy** • Security is guaranteed by national governments, criminal prosecution on national level • No interaction between security policy and other policy areas • More emphasis is put on defence than on trust • Tendencies to harmonise the legal framework are given up; strong influence of lobbies	
2	**General develop-ment of EU**	**2A | Strong development of Europe and further integration** • Europe's development performs well; People feel as EU-citizens • Strong appearance of the EU in global affairs • Further EU enlargement, political & monetary • Advanced harmonisation • Consensus on important policy fields	**2B | EU of different nations and different integration levels** • EU is divided in different regions and characterised by different integration levels • EU enlargement aimed, whereas the euro zone is minimised • Harmonisation is unchanged, compliance is more relevant in the industry/economical sector than in politics • Growing mismatch between local responsibility and European participation; Decreased political influence of the EU worldwide	**2C | Decreasing importance of EU** • Return to the interests of nations and regions, EU is hardly capable of making decisions • EU enlargement is stagnating • Harmonisation is given up; structures for compliance are missing • Bankruptcy of several member states threatens the monetary union • People do not feel as a part of the EU	**2D | European political union with new constitution** • Political European Union by EU enlargement, new constitutional treaty • Harmonisation is completed; the position of EU institutions is reinforced • Despite of the internal liberalisation of the EU, 'closed' external borders • Shifting all fiscal and economic policy powers from the nations to the EU

3	**EU R&D infra-structure**	**3A | Public funding scheme** • Equal & legal financial treatment of all types of partners (industry/ research institutions - public/ private) • Stronger interrelation of European and national research programs (priorities, dissemination, standardisation) • EU instruments for supporting R&D cooperation are successful • International R&D cooperation is strengthened	**3B | Mix of public & private funding** • Security research is financed by the EU as well as by nations, but larger proportion of private financing • Increased competition between public and private R&D actors • Internationalisation and cooperation are crucial for national research programs	**3C | Shift to private R&D funding** • Less EU funding for security research, shift to private funding in R&D • Private as well as public institutions • Insufficient harmonisation • Circulation of research is still complicated, member-state-specific rules • Multiple research financing, overlaps in research activities and unnecessary duplicated research	**3D | Shift to private funding and research** • No more EU funding for security research • R&D funding and research in private institutions and private universities • A few big players dominate security research • Individual funding determines R&D, leads to research overlaps as well as unnecessary duplicated research
4	**Commer-cialisation strategy of R&D**	**4A | EU-Security label & far reaching information providing** • European security labels are established • Public sector information for security technologies and policies are easily and timely accessible • Specialised training concepts for new systems and technologies • R&D and scientific results are freely accessible and provided, this supports the acceptance of new security technologies	**4B | No security label, but marketing label & limited public information** • Information providing is lead by market and business interests, limited public sector information • User integration in the technology development process is smaller, yet companies offer training concepts for new system technologies	**4C | No security label & few/less public information** • Neither a security nor a marketing label • Only fragmental information is provided to public sector, what reduces trust in security technologies and systems • Improper use could lead to security risks	
5	**Design and orientation of R&D**	**5A | Resilience-driven R&D** • Shift of the orientation: not to prevent the risk but accept and propose for it • EU and national security research and innovation focuses on strengthening resilience of society	**5B | Threat-driven R&D** • Dual use of research results (civil & military) • Security research is threat driven technology research • Focus on securitisation of life		

6	**Capabilities & capacities in R&D**	**6A | European human resources are sufficient** • European human resources are sufficient • Operational immigration policy • Attractive jobs are offered • Europe has technological, industrial and scientific competences	**6B | Lack of EU-talents & recruitment outside Europe** • European human resources are not sufficient • International recruitment is successful, attractive jobs in Europe • General shortage of well educated, talented young people	**6C | Lack of EU-talents & international recruitment failed** • European human resources are not sufficient, lack of talents • International recruitment has failed • Specialization and focusing on core research fields takes place • Research activities are shifted to institutes outside Europe	
7	**Design and implemen-tation of security technolo-gies**	**7 A | Orientation on user-needs and convergence** • Society is actively involved in the technology development and innovation process • Convergence and interoperability are widely standardised • Innovation speed is lower, quality insurance is important • Synergies between stakeholders, technologies and services	**7B | Competition-driven and user-independent** • Influence of the society on technology development and innovation process is lower • Technology development usually does not meet user needs • Heterogeneous technology landscape impedes interoperability and standardisation • Higher innovation speed; Quality assurance is complicated		
8	**Security understanding and concerns in society**	**8 A | Declining need for security** • Political and economic stability reduce the need for more security • Risk awareness of the society is sinking due to the declining need for security	**8 B | High need for more security** • Due to demand of high security levels, public acceptance is given • For higher security level citizens reduce the claims to their fundamental rights	**8 C | High risk awareness** • Security perception is determined by risk awareness • Penetration of life through 'security' technologies is adequate; As moral courage is a ruling principle society is very self-confident	

9	**Cultural influences and social change**	**9 A | Great significance of social value system** • Active ageing, life-long education, demographic change and new living models play a significant role • Increasing public awareness and sensibility for any type of unfairness and injustice • Heterogeneous landscape of different religions and beliefs • The 'western' value system remains important in the European countries	**9 B | Changing value system and focus on material interests** • Material interests more important than traditional and social values • Strong demographic change • The social gap grows further and there is a strict differentiation between social classes (e.g. Gated Communities) • Extreme groups become stronger and difficult to control		
10	**Attitude towards technolo-gies in society**	**10 A | Acceptance depends on user friendliness & scrutinizing** • Technology acceptance differs depending on its characteristics (> suitable for daily use) • Strong focus on user friendliness • Virtualization may lead to new levels of social "digital" competences	**10 B | Technology-hype & no scrutinizing of research** • High technology penetration of everyday life, trust in technological solutions • Expansion of virtual communities of interest groups (e.g. church, political parties,...) may have an impact on opinion making, complicating the ability of states to govern	**10 C | Decreasing technology acceptance & scrutinizing** • Technology acceptance is decreasing in general • (Security) technologies in general are assessed rational • People scrutinize research findings • Effective and efficient research is required • Digital divide	
11	**Global economical arrange-ment**	**11 A | Long-term stability & quantitative growth** • Worldwide long-term economical stability and worldwide recovery of business activities • Budgets of EU member states are robust • EU is competitive • Globalization and integration of emerging countries	**11 B | Instable economic situation, emerging new economies** • Instable economical system and many crisis • Many hotspots • Economical aspects take priority over sustainability • New global players evolve (Brazil, Argentina, China, …)	**11 C | Long-term financial crisis and global instability** • Long-term financial crisis is still not overcome • Permanent regional crisis reach global impact • Few prosperous regions • National focus results in conflicts over markets, investment flows and resources • Attention on fiscal gaps and many countries risk unsustainable debt levels	**11 D | Long-term stability & qualitative growth** • Worldwide long-term economical stability • EU member states and the EU have robust and stable budgets • Public budgets are used efficiently • Orientation towards qualitative growth and benefit • Globalisation and the integration of emerging countries into the world economy proceeds

12	Production and consum-ption behaviour	**12 A | Efficient and sustainable** • Global rethinking • Sustainable production • Rapidly changing production and process patterns • New forms of value creation • High awareness of sustainability	**12 B | Inefficient and un-sustainable** • Production modes differ between regions depending on access to natural resources • Increased focus on core competences and outsourcing (relocation of production and competences) • Awareness of sustainable consumption, but economic aspects are more important than sustainability		
13	Security industry	**13 A | Global leadership of EU by knowledge-based security industry** • Europe has strong extensive industrial capability and knowledge base in the security field • Customized security solutions, more interaction between supply and demand • Strong alliances between policy and industry	**13 B | Strong security industry by fragmented market** • Strong extensive industrial capability and knowledge base in the security field • Market is fragmented • Efficient European industry • Missing overarching dialogue between policy makers and security industry	**13 C | Big players, focus on market-driven interests** • Multinational companies determine the market, focus on markets with few risks • US comp. dominate the security market • Gap between supply and demand (private, public, industry) • Dialogue between industry and policy is complicated and interest driven	
14	Relevance of security in different sectors	**14 A | Security economy - risk acceptance** • Security economy is oriented towards risk awareness • The supply of and demand for security technologies is decreasing and determined through usefulness • Vulnerability decreases but still exists	**14 B | Security economy - fully secure** • Security economy is oriented towards fully controllable technologies; very high security level aspired • Security technologies are everywhere irrespective of usefulness (demand and supply) • Vulnerability increases		

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	
		• Open knowledge - knowledge is seen as common property • Rare granting of exclusive patents • Open Source, Open Data and Crowd Sourcing • Working on common standards	• European harmonisation, Member states agreed upon EU patent; Actions depending on the sector (e.g. Software) • Protection of knowledge is important, confidential handling of knowledge	• No harmonisation on EU level; National laws dominate in the field of IPR • Multiple patent applications are necessary for protection; 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
		• Absence of great power conflicts • Community of states • Economic prosperity and growing acceptance of democratic norms • Security is handled on global level • Resource scarcity are met effectively • Sustainability and green footprint	• Tensions between regions, states and national identities • Political systems competing • New emerging states and powers • Balance of military powers shifts to various regions • Greater demand and competition for essential resources	• Hegemonic aspirations of several countries • Persistent danger of terrorism • Non-military aspects of warfare gain more importance • Growing worldwide demand for energy and fossil fuels • Major resources are in politically unstable regions • Some countries will fall further behind	• Political global scene is dominated by regionalism; growing protectionism • Conflicts over markets, investment flows, and resources • International collaboration on terrorism, crime, cross-border conflicts reduced • High conflict potential in Failing States • Benefits of technologies will be realised by only a few 'rich' countries
17	Global emergencies and disasters	17 A | Overwhelming international system	17 B | Interest-driven interventions	17 C | Underinvestment of infrastructure	
		• Persistent danger of humanitarian emergencies / natural disasters • Coordinated, effective and efficient Crisis Management • Interoperability at the communication level • Globalisation of Crisis Management	• Increased risk of humanitarian catastrophes • "Justification" for interests-driven military interventions • Militarisation of Crisis Management	• Growing risks of humanitarian catastrophes • Vast segments of water, energy or transport infrastructure are structurally deficient / functionally obsolete • Rivalry between military and civil protection forces	

Table 9: Key factors and future projections of context scenarios
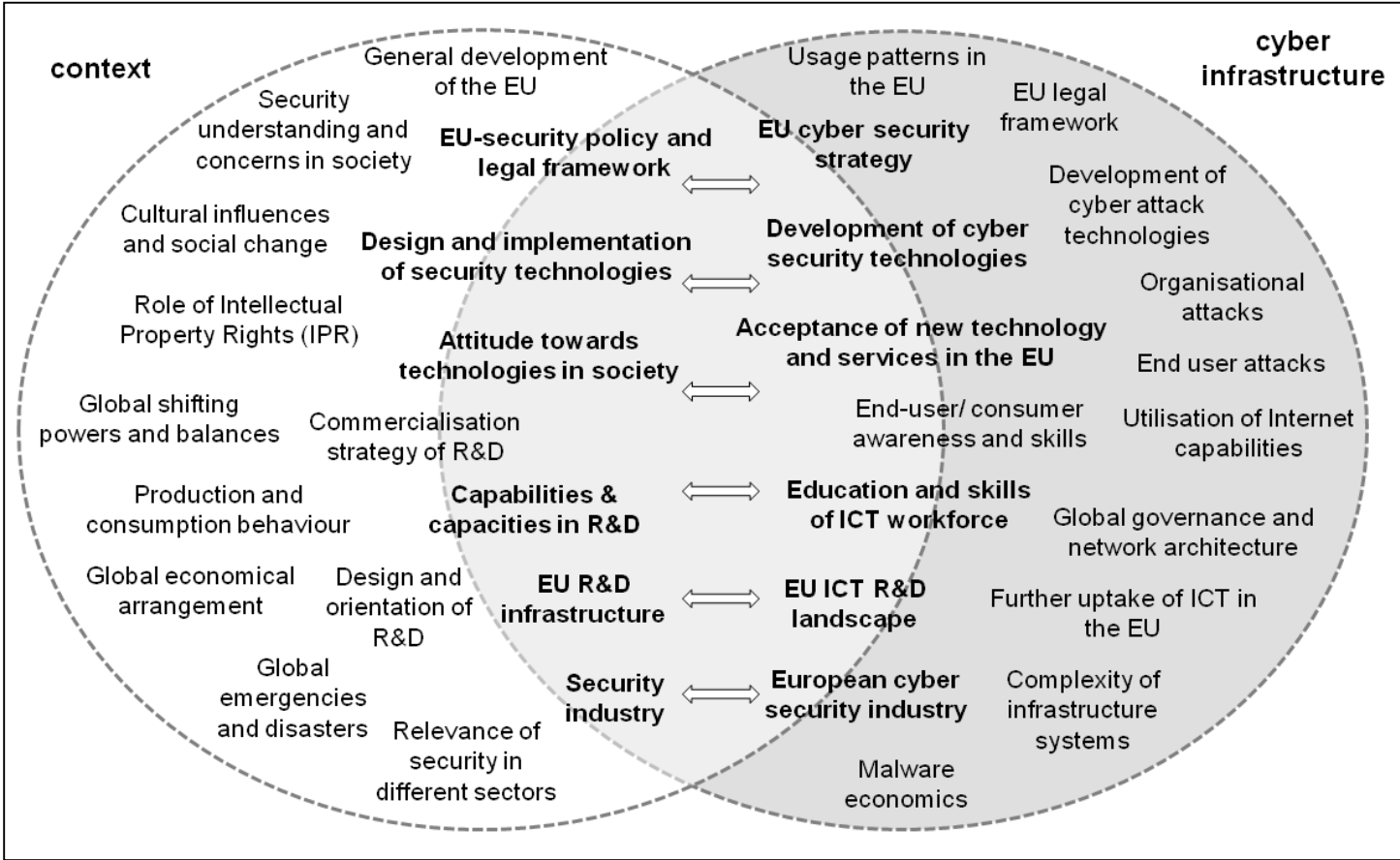
6.1.2 Cyber infrastructure

Figure 20: Linking context and cyber infrastructure

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** • Return of national governance structures • Architectures' increasingly modified according to national priorities (f. e. kill switch architectures) • No further regulation of cyber war fare • No cooperation on cyber crime and terrorism	**C1B | Private sector led governance** • Independent, international governance structures by private organised bodies • New approaches to overall network architecture mainly based on market driven approaches • Official aim of cyber war and related activities by nations, but private activities remain (economic espionage) • Strong private driven international cooperation on cyber crime, less attention to cyber terrorism	**C1C | Fragmented governance in existing structures** • Different governance modes for different parts of cyber infrastructure • Existing architectures principles remain, only modest modifications of different security issues • Regulation of cyber warfare comparable to other warfare regulations • Singular cooperation on cyber crime and terrorism (limited to specific topics or forms of attack)	**C1D | Integrated governance and new architectures** • Independent, international governance structures by international bodies • New approaches to overall network architecture based on security principles and interoperability • Ban of cyber war and related activities by nations • Strong international cooperation on cyber crime and terrorism
C2	**Complexity of infra-structure systems**	**C2A | Complexity as a mess** • Growing entanglement of cyber infrastructures and other infrastructures • Risk of cascading effects grow • Legacy systems form great security challenge	**C2B | Complexity as management challenge** • Entanglement of different infrastructures • Measures to reduce impacts of cascading effects • Active policy to replace legacy systems or at least to upgrade them	**C2C | Avoidance of complexity** • Punctual connection between cyber and other infrastructures • Minor risks of cascading effects • Legacy systems form still a challenge, but avoiding to integrate them	
C3	**EU legal framework**	**C3A | Fragmented regulation in EU** • Differentiated legislation on data protection and privacy across the EU • only limited cooperations on national level between EU member states • no future orientation • lack of effective measures for prosecution and prevention	**C3B | Strong, but ineffective framework** • Strong EU wide legislation on data protection and privacy • Framework too strict and leads to overregulation • High expectations on strong institutions, but they fail • Development influenced by strong industrial lobbies	**C3C | Strong common framework for the EU** • Strong EU wide legislation on data protection and privacy • strong EU institutions ensuring cooperation in relevant areas like crime prevention and prosecution • future oriented framework anticipating societal developments • balanced mixture of prevention and prosecution, incl. penalties and fines	

C4	**EU Cyber security strategy**	**C4A | Non-coordinated approach** • Lack of co-operation between member states and EU • Different types of exclusion and inclusion of stakeholders • Lack of clear focus regarding threats • Different approaches towards strategy	**C4B | Defense oriented approach** • Focus only on security critical actors, i.e. exclusion of civil society • Defence as a major principle • Less focus on basic human rights	**C4C | Coordinated strategy focussing on resilience** • Strong coordination through public private partnerships to increase protection level • Resilience as main principle of the strategy • Strong focus on human rights	**C4D | EU as global leader in cyber** • Strong coordination through public private partnerships to increase protection level • Strong focus on leadership in cyber technologies • EU pushes standardisation and interoperability as tools
C5	**Develop-ment of cyber security technologies**	**C5A | Security theatre** • Strong development of security technologies • Users can't deal with • Efficiency unknown	**C5B | The hedgehoc and the hare** • Security technologies always behind threats, reactive patterns • Normally patch-driven culture • User often let alone	**C5C | Towards proactive security technologies** • Focus on proactive technologies • Fast advances of cryptographic methods • User friendliness as priority	
C6	**Develop-ment of cyber attack technologies**	**C6A | Attack as the best defense** • Increased spending on attack technologies • Attacks as a permanent part of the cyber strategy	**C6B | Attack – only if we can deny it** • Attack technologies were developed, but mostly in the dark • Officially attacks are only limited part of the strategy	**C6C | Decline of attack technologies** • Attack technologies are banned • Only few nations still try to exploit	
C7	**EU ICT R&D landscape**	**C7A | Heterogeneous R&D Landscape** • Low public investment into ICT R&D infrastructure • Unclear and unstable financing mechanisms, partly joint financing, partly national and private • Low coordination of research strategies	**C7B | Homogeneous R&D Landscape** • Sufficient public support for ICT R&D • Coordinated and stable financing (EU and member states; public and private) • Involvement from other areas, experts and policy increase synergies of R&D efforts		

C8	**European cyber security industry**	**C8A | Globalized world** • End of the US dominance • Rise of new players in cyber security all over the world, including EU and BRICS • Increasing international co-operations between suppliers	**C8B | Foreign domination** • Dominance of non-European players, mainly US players in cyber security • EU player only exist in few market niches	**C8C | EU security industry gain of importance** • European player ascend among the major players in cyber security • EU cyber security industry capable of responding to most of the threats regarding cyber infrastructure security	
C9	**Further uptake of ICT in the EU**	**C6A | Stagnation of diffusion** • Uptake of Internet of X only takes place in selected areas • Connectivity increases in the EU, but slower as in other world regions • Only punctual digitalisation of processes in business and public services	**C6B | Slow down of diffusion** • Strong barriers for advanced web services leading to a delay of the Internet of X • Slow, but progressing digitalisation of processes in business and public services • Internet access differs strongly between regions in the EU	**C6C | Enforced diffusion of ICT** • Breakthrough of advanced web services enforces deployment of Internet of X • Increased digitalisation of processes in business and public services • High bandwith (FTTH or similar) access are common in the EU	
C10	**Acceptance of new technology and services in the EU**	**C10A | Forced penetration with low acceptance** • Growing penetration of new services, mainly forced by work and other factors • People use, but distrust these new services • Acceptance of internet technologies declines • Different level of risk tolerance by industry and consumers	**C10B | Growing reluctance against new services** • Growing distrust of users towards internet services • General low acceptance of internet technologies • Low risk tolerance by industry and consumers influencing acceptance negatively • Delayed take up of new services	**C10C | Open society embraces digital technologies** • Strong trust in internet services • Trust in measures for protection because of openness • Risk tolerance not essential anymore for attitude towards single services • Fast uptake of new services	**C10D | Deliberated acceptance** • Awareness of chances and challenges • Trust and security only in specific internet services • Consistent use of services/tools • Differentiated risk tolerance • Balanced uptake

C11	**Usage patterns in the EU**	**C11A | Hybrid models of usage** • Strong adoption of Cloud services by industry, governments and consumers • Benefits for many, but not for all user • Limited numbers of players, but no dominance of single providers	**C11B | Dark Clouds** • Adoption of Cloud services vary strongly between the different groups • Benefits only for a few user, in particular due to economies of scale • Strong dominance of few suppliers influencing competition negatively (lock-in)	**C11C | Up in the air** • Massive adoption of Cloud services by industry, government and consumers • Competitive markets in Cloud services • Benefits for a broad group of users	
C12	**End-user/ consumer awareness and skills**	**C12A | Fragmentation of user groups grows** • Digital divide between professional user and the rest grow further • Measures to increase literacy fail in large scale	**C12B | Digital natives take control** • Digital natives are much more aware of challenges and chances • Growing experience with internet technologies • Forces industry to more user friendly solutions	**C12C | Increasing awareness** • Divide between different user groups decrease • Massive efforts to raise awareness and literacy • Strong efforts to increase usage and usability of security tools	
C13	**Education and skills of ICT workforce**	**C12A | Mixed developments** • Increasing number of workforce, but quality of workforce vary strongly • Lifelong learning only minor focus • Strong fight for the best in the industry	**C12B | Stagnation of workforce** • Number of workforce stagnates • Skills improve due to quality measures and focus on lifelong learning • Active measures to keep quality of workforce due to shortage	**C12C | Increasing capabilities** • More and better educated workforce • Focus on lifelong learning to keep pace with fast developments • Industry needs can be satisfied	
C14	**Utilisation of Internet capabilities**	**C14A | Only crime utilize** • Growing exploitation by cyber crime • Low usage of capabilities for prevention and prosecution • Low risk of detection for criminals	**C14B | Strong utilisation in all areas** • Growing exploitation by cyber crime • high usage of capabilities for prevention and prosecution • high risk of detection for criminals		

C15	End user attacks	C15A | Scaling up of attacks • More attacks on normal users take place • Level of threat also increase (not only phishing) • Countermeasures are non-effective	C15B | Diversity increases • More attacks, but strong diversity of the level of attacks • Increase in both, specific, more intelligent attacks on specific user groups as well as mass attacks • Countermeasures help in the first case, latter they fail	C15C | Stagnation and decline of attacks • Strong international cooperation to stop cyber crime • Consequently number of attaks decline • Economics of such attacks become worse due to effective countermeasures, i.e. threat of detection and prosecution increases	
C16	Organiz-ational attacks	C16A | More sophistication • More targeted and specific attacks on organisations • Usage of very sophisticated, complex attack technologies • Number of targets increase trough more diffusion and convergence	C16B | Divided worlds • Advances in security exist, but only affordable to few rich organisations • Number of attacks increase • low risk of detection	C16C | Increased countermeasures • Advances in security are faster then the one of the attackers • Although number of attacks increase, success rate decline • Higher risk of detection	
C17	Malware economics	C17A | Creation of a malware industry • Governments and industry start to buy exploits in large scale • No open policy regarding known exploits • "Better sell than tell" become usual in the scene	C17B | Black stays black • No deals between industry or governments and malware producers • Hacker ethics prevail: exploits need to be published • Open policy of industry regarding known exploits		

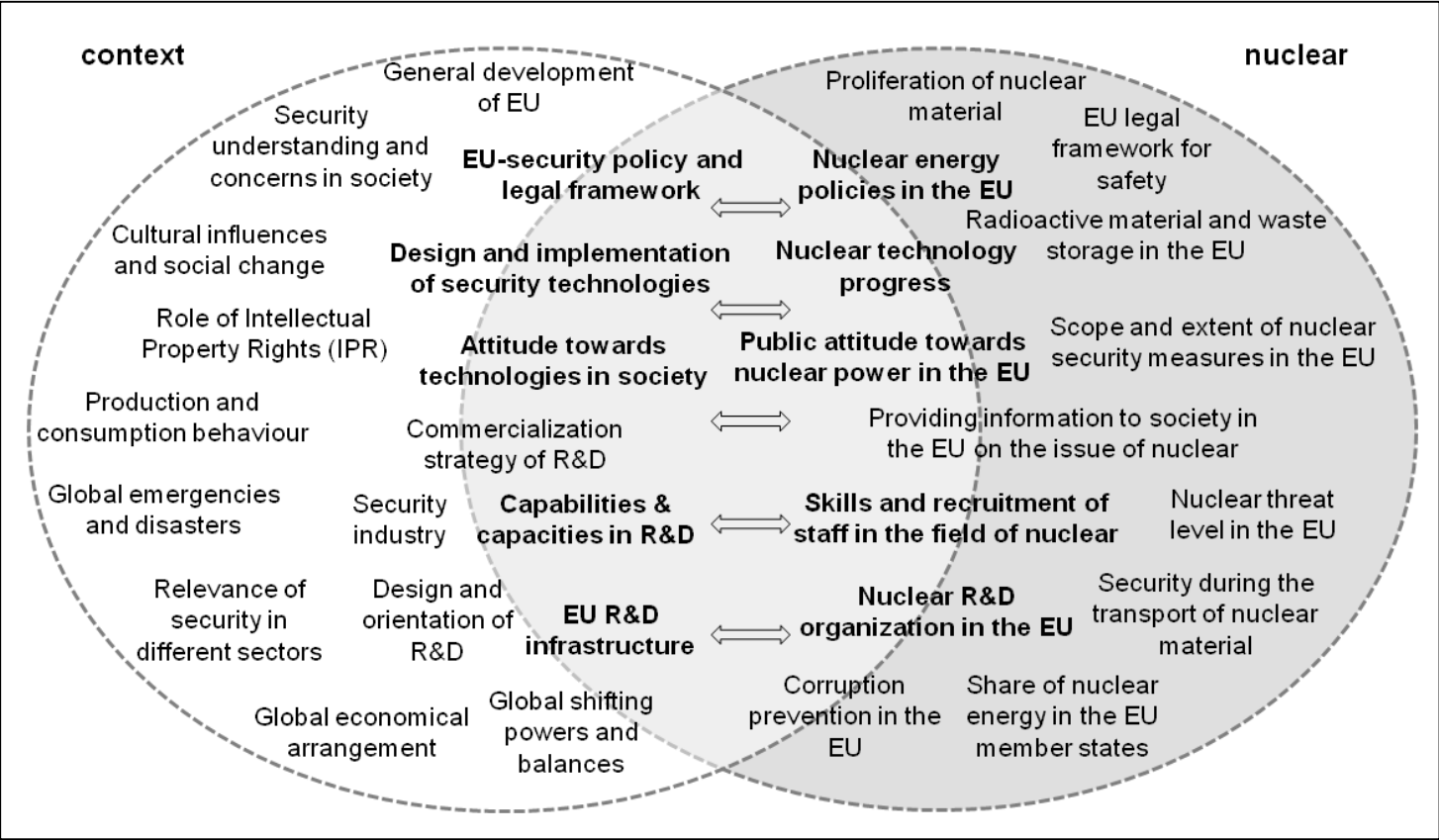Table 10: Key factors and future projections of cyber scenarios

6.1.3 Nuclear

Figure 21: Linking context and nuclear

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** • High interaction between nuclear energy policy, security policy and other policy areas, like environmental policy or fiscal and financial policies. The nuclear energy policy is also linked to other important issues for the EU: climate change; regeneration; world toxic waste exports • Harmonized energy strategy	**N1B | National focus of nuclear energy policies** • Interaction between security policy and other policy areas on EU-level is limited • No framework or agreed strategic approach as well as real long term strategic thinking (100y+) • Tendencies to harmonize the energy strategy are given up; strong influence of lobbies		
N2	**Share of nuclear energy in the EU member states**	**N2A | Increased nuclear energy French way (pro)** • 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 • Economic viability of nuclear power is given • Mechanisms for encouraging nuclear power (on the European level or national level) are established	**N2B | Stagnation of nuclear energy Situation like today** • 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 • Nuclear power addresses security of supply only in some countries • Only the member states have programs in favor of the nuclear power and sufficient mechanisms for encouraging nuclear power	**N2C | Decline of nuclear energy German way (anti)** • No assistance programs (on the European level or national level) • Significant investments in improvement of the power plants were not made, while the existing reactors are going to retire (high cost of shutting down) • No assistance programs (on the European level or national level)	

N3	**Nuclear technology progress**	**N3A | Progress in identifying options for nuclear fuel cycle** • More solutions for sustainable fuel cycle, like reducing waste due to improving resource utilization (recycling and reuse of uranium and plutonium) • High-performance computing for integrating theory and experiment with modeling and simulation • Evolution to reactor generation III and IV	**N3B | Progress in alternative technologies** • No technology progress in nuclear fuel cycle • Leading to a breakthrough in nuclear alternative technologies (like Fusion, solar, fracking)	**N3C | Less technology progress in nuclear fuel cycle** • No long-term prognosis for behavior of the radioactive material of the castor storage • Insufficient development of sustainable technologies, which reduce waste due to improved resource utilization (recycling and reuse of uranium and plutonium)	
N4	**Nuclear R&D organization in the EU**	**N4A | Distributed R&D Landscape - EU and national level** • Underinvestment of R&D infrastructure • Joint financing (EU and member states; public and private); the share is not clear defined • Less synergies between stakeholders	**N4B | Joint R&D Landscape - EU and national level** • Joint financing (EU and member states; public and private) • Involving experts within and outside the traditional nuclear field, like nano science • Involvement of policy makers and industry as a necessary partner	**N4C | Distributed R&D Landscape – No R&D at EU-Level** • Investment of R&D infrastructure driven by national interests • Public financing by EU member states at national level; private financing in some cases also initiated by international commitments	
N5	**Skills and recruitment of staff in the field of nuclear**	**N5A | Knowledge pool in Europe** • Europe has technological, industrial and scientific competences (nuclear power plants and R&D in the flied of nuclear material) • Attractive jobs are offered; also nuclear waste management is seen as 'green' and attractive	**N5B | European human resources are not sufficient** • Small community of nuclear experts • Specialization and focusing on core research fields takes place (most popular research fields, like nuclear waste management) • Networking – access to specialized skills and knowledge in countries outside Europe	**N5C | Great lack of high qualified staff** • General shortage of well educated, talented young nuclear experts • Integration of nuclear waste management skills and knowledge in general waste management	

N6	EU legal framework for safety	**N6A | European regulation and harmonization: legislative approach** • Advanced harmonization and regulation, but structures for compliance are missing • Regulatory harmonization and licensing process of nuclear power plants at the EU level are successful • Safety and security must be integrated from the earliest stage of the design • Obligation to reviewing all EU nuclear power plants by national regulatory bodies and peer review on the basis of a comprehensive and transparent risk and safety assessment ('stress test') still exist	**N6B | International regulation and harmonization: compliance based approach** • More compliance with regulations: Voluntary recognition, Mutual recognition (a plant type licensed in one country should be accepted in any other EU country) • Legislation based on consultation with a group of experts, public consultation, consultation of the European Nuclear Safety Regulators Group (ENSREG) • Design licensing regulations based on the consultation with communities from industry to reflect on possible approaches ENSREG and Multinational Design Evaluation Program (MDEP)	**N6C | National regulations within EU** • Safety regulation at national level by national regulatory agencies • Differences in the licensing of new nuclear power between member states, which may result in lower levels of nuclear safety, reduces efficiency for all actors, increases regulatory uncertainty for investors • There are also international commitments, but mainly without compliance and sanctions, thus practically not effective	
N7	Scope and extent of nuclear security measures in the EU	**N7A | Ambition of ensuring all over security - precaution** • Ambition to cover all (thinkable) threats • Lessons learned from previous actions or incidents, like diversity of IT-solution (i.e. digital/analog)	**N7B | Ensuring all over security not possible - realism** • Not all threats are thought and not all known or anticipated threats are covered • Deterioration of security culture		

N8	Radioactive material and waste storage in the EU	**N8A | Final European repository** • Joint waste management in an European centralized geological repository (or few repositories) • Public responsibility for disposal • Joint financing scheme: member states and EU • Long transport distances to the centralized facilities	**N8B | Final central repository at national level** • Most countries have one final repository underground as an efficient solution at national level • Financing at national level • Public responsibility for disposal • Longer transport distance between storage in power plants and final storage • Individual nuclear waste legislation in each country • Orientation on common EU standards for disposal, but no obligation	**N8C | Central interim storage facility at national level** • Centralizing all radioactive material and waste generated in an interim storage facility as an efficient solution at national level • Financing at national level • Mainly public responsibility for disposal • Longer transport distance between storage in power plants and interim central storage • Individual nuclear waste legislation in each country	**N8D | Short-term national interim storage facilities** • Financing at national level • Confusion concerning the responsibility for disposal: private (in nuclear power plants) vs. public (elsewhere) • Sites with low local resistance are preferred over those with best geological conditions • Confusion concerning the responsibility for disposal: private (in nuclear power plants) vs. public (elsewhere) • Individual nuclear waste legislation in each country

N9	Security during the transport of nuclear material	**N9A | Ensured safety and security**
		
		• Regulated and structured transport:
		  • Joint responsibility
		  • Integration of different stakeholder and experts
			N9B | Insufficient safety and security
			
			• High priority to ensure safety and security over the radioactive waste during transport, but without practical success		

N10	Proliferation of nuclear material	**N10A | No change of measures for non-proliferation** • 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 • Mostly clear distinctions between civil and military use of nuclear power	**N10B | Insufficient monitoring measurements of non-proliferation** • Difficulties of enforcing international treaty obligations • New sources of proliferation: Widespread use of nuclear technologies in new countries with very diverse systems • Expansion of the civilian nuclear sector (lack of strict monitoring or security arrangements) • No clear distinctions between civil and military use of nuclear power in some countries	**N10C | Improvement of the non-proliferation safeguards** • Stronger international regulation and control (i.e. diversion of nuclear material was involved) • More countries joined the Nuclear Non-proliferation Treaty (NPT) and renounced nuclear weapons to enhance national security. • More nuclear facilities are declared or placed under safeguards arrangements	

N11	**Providing information to society in the EU on the issue of nuclear**	**N11A | Public driven approach** • Far reaching, but interest driven information providing, driven by country policies or policies of the EU (e.g. energy policy or environmental) • Public responsibility approach for information providing involving the EU and the European countries concerning e.g. security technologies or risks • Mix of public and private funding to secure availability of capacity of resilience; private share is lower	**N11B | Market driven approach** • Information providing is lead by market and business interests, thus limited public sector information about risks • User integration in the technology development process is smaller, yet training concepts for new system technologies exist • Mainly private founding to secure availability of capacity of resilience (limited to particular sectors or for a certain region)	**N11C | Partnership approach** • Far reaching information providing • New communities, like society representatives or environmental communities are involved for including new perspectives • Public and private responsibility approach for information providing • Importance of security culture, thus also measures for education and training • Mix of public and private funding to secure availability of capacity of resilience; private share is lower	
N12	**Public attitude towards nuclear power in the EU**	**N12A | Acceptance differs from region to region** • Acceptance differs between EU regions (or member states) • Higher level of support for nuclear energy in EU nuclear countries compared to EU non-nuclear countries	**N12B | Overall decreased acceptance** • Society less or not involved in decisions about the nuclear power policy • No trust in institutions, which provide information	**N12C | Wider acceptance** • Society is directly involved in decisions about the nuclear power policy or construction of underground disposal sites (or indirectly by representatives) • Awareness of the advantages of nuclear energy and of the safeguards in place • Trust in institutions, which provide information	

N13	**Corruption prevention in the EU**	**N13A | Ambiguous responsibility – national vs. EU-level**
		
		• Ambiguity relating to the responsibility for the combating of corruption and fraud (national or EU-level?). However the responsibility is most private owned:
		  • Decreased collaboration on crime between European Countries
		  • The criminal prosecution concentrates on national level
			N13B | Responsibility at national level
			
			• Responsibility for the combating of corruption and fraud almost exclusively at the national level (public or private)
			  • Less collaboration on crime between European Countries
			  • No overarching solutions
				N13C | Joint responsibility
				
				• Strong responsibility for the combating of corruption and fraud, public as well as private:
				  • Cooperation is welcomed and usual; good international (EU countries) collaboration on crime
				  • Overarching solutions are found, communicated, and are efficient	

N14	**Nuclear threat level in the EU**	**N14A | High level of threats** • New countries involved in nuclear sector and proliferation; No safety regulations in these countries • Nuclear waste becomes a „currency" and has criminal value • There are strong protest groups and violent actions and opposition demonstrations • High corruption level	**N14B | Moderate level of threats** • Unforeseen incidents, like theft or terrorists attack still happen • There are protest groups and opposition demonstrations • Corruption and fraud increased	**N14C | Low level of threats** • Unforeseen incidents, like theft or terrorists attack still happen • There are still some protest against the nuclear power and opposition demonstrations • Corruption still exists	

Table 11: Key factors and future projections of nuclear scenarios
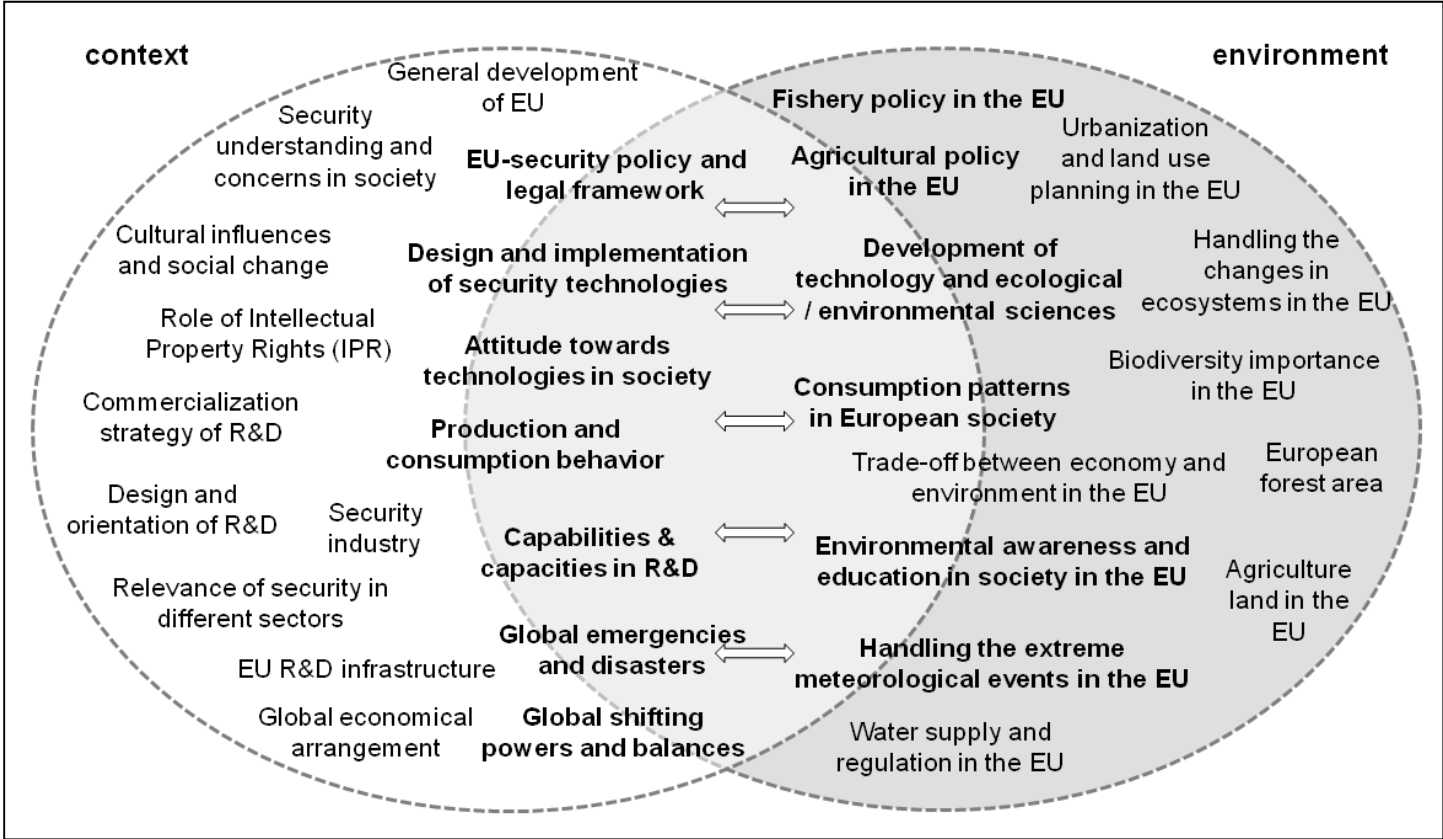
6.1.4 Environment

Figure 22: Linking context and environment

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** • Increased consumption of agricultural products and higher worldwide electricity demand • Increasing demand for livestock products. Food consumption patterns significantly impact water requirements.	**E1B | Increased consumption with adapting towards more sustainability** • Increased consumption of agricultural products and higher worldwide electricity demand • Consumption shifts gradually to a more sustainable direction: More importance about consumption of vegetable matter; Healthy and targeted nutrition	**E1C | Stagnating consumption without a change in behavior** • Stagnating or decreased consumption of agricultural products, but higher worldwide electricity demand • Increased awareness of linkage between consumption and environmental problems happens gradually, but economic aspects are still more important than sustainability	**E1D | Stagnating consumption with adapting towards more sustainability** • Stagnating or decreased consumption of agricultural products: healthy eating patterns, moving towards plant-based diets and towards a reduced consumption of meat (i.e. alternative food like insects) • Awareness of local or global consumption (Environmental justice)
E2	**Environmental awareness and education in society in the EU**	**E2A | No focus on environmental education, less environmental awareness** • Generally less interest in environmental aspects as well as biodiversity and ecosystem characteristics and services, only partly environmental awareness • Limited and market driven information providing concerning e.g. effects of chemicals, pesticides or risks from biodiversity loss • No implementation of the EU strategies for sustainability	**E2B | Raised awareness, but no own responsibility or action** • People become more sensitive towards environment. A high quality of life through a healthy environment is increasing in esteem, but the environmental education is still not keeping pace with environmental degradation • More information about environmental aspects provided to society; Public responsibility approach • No implementation of the EU strategies for sustainability	**E2C | Higher environmental education with responsibility for environmental problems** • More and more people are aware of the values of biodiversity and the steps they can take to conserve and use it sustainably • Partnership approach of Information providing, involved governments, EU, business sector and society for the benefit of communities as well as operators • Implemented EU strategy for Sustainable Development with priority areas like climate change and clean energy, sustainable production and consumption, conservation and management of natural resources	

E3	**Agricultural policy in the EU**	**E3A | Effects of the CAP reform insufficient** • CAP (Common Agriculture Policy) doesn´t meet the environmental and social challenges: Still lack of regulation of markets and production; Large expansion in agricultural industrial production (global, cheap production instead of regional high quality production) • No improvement definition, who is an active farmer	**E3B | Reformed CAP spreads its positive effects** • Simplification of the agricultural policies, especially maintaining solid financial management and controllability • The direct payments to farmers are more equitable and balanced between Member States and farmers and better targeted at active farmers (small and large range); • Improved definition, who is an active farmer	**E3C | New Common Food and Agriculture Policy with food sovereignty** • Changes in international trade in agricultural products according to principles of equity, social justice and ecological sustainability • Fair and secure farm prices as well as prices for consumers • Promotion of the production and consumption of local, seasonal, high quality products reconnecting citizens with their food and food producers	
E4	**Development of technology and ecological / environmental sciences**	**E4A | Chemical and nutrient pollution for more efficiency** • Insufficient development of sustainable technologies and lack of innovation in food production • Use of chemical fertilizers, herbicides, and pesticides which may cause diseases. • There is still no clear evidence on the effects of the consumption of genetically treated food	**E4B | Innovations in food production** • Modern crop varieties; Biotechnologies in the production of feedstock for industry, in production of functional food, biotechnological applications such as seeds or bio pesticides; Innovations in food packaging and food distribution • Using of urban zones for new forms of sustainable, viable, food production (e.g. urban gardening, bringing together small-scale producers)	**E4C | Efficiency and sustainability of novel agricultural systems** • Sustainable scientific focus on the dynamic interactions between nature and society • Innovations concerning perishability and shelf life of agricultural products • Other technologies used in agricultural production (beside the biotechnology), like nanotechnology • Agroecological Engineering: e.g. habitat management techniques (e.g. biological pest control, beetle banks around wheat fields), or natural agriculture systems aiming at perennial food-grain-producing systems (e.g. organic farming)	

E5	**Trade-off between economy and environment in the EU**	**E5A | Relationship economy vs. environment got worse** • There are still conventional economic aggregates generated through national accounting, such as GDP without reflection the extent to which production and consumption activities may be using up environmental assets and limiting the capacity to generate ecosystem services in the future • No measurement of environmental loss: Environmental degradation is still largely treated as an externality.	**E5B | Higher significance of nature-compatible economies** • Economic accounting using indicators regarding economic development as well as environmental sustainability are relevant in tracking country progress. • Ecosystem services as an economic factor (instruments for calculating of follow-up costs of loss of services) • Nature-compatible production: Regarding the environmental aspects by the management of companies gained more and more importance	**E5C | Trade-off changes slightly in favour of the environment** • A gradual, but slow awareness about the real costs of nature degradation • The externality concept will be reassessed: Environmental degradation is not just an externality. • An increasing awareness of corporate social responsibility among investors and companies • Appropriate instruments for calculating of follow-up costs of nature degradation ("Authority of evidence")	
E6	**Handling the changes in ecosystems in the EU**	**E6A | Less interventions for ecosystem protection** • There is still less understanding of the factors that cause changes in ecosystems and ecosystem services and unclear how dramatic the changes in ecosystems are going to affect us. • Less interventions that enhance positive and minimize negative impacts of the degradation of ecosystem services • Unclear responsibilities: public and private decision-makers at municipal, provincial, and national levels/ international level	**E6B | Measures for ecosystem protection at local level** • Measures at the local/ regional level, which directly influence e.g. the choice of technology, changes in land use • There are still diffuse approaches for handling the ecosystem changes at the European level	**E6C | EU measures for ecosystem protection implemented** • Better protection and restoration of ecosystems and the services they provide, and greater use of green infrastructure. • Measures at the European level, which influence e.g. prices and markets, property rights, technology development, or the local climate • Introduction of economic instruments (e.g. payments for ecosystem services, conservation offsets, conservation banking, pricing, taxes, charges, subsidies, tradable permits, removal of perverse subsidies and incentives)	

E7	**Handling the extreme meteoro-logical events in the EU**	**E7A | Slow adjustment to increased extreme weather conditions** • Partially no lessons learned resulting in high external costs of extreme meteorological events or natural hazards, mostly at the local level • Mistaken investment decisions (also allocation of the EU funds) after previous events leading to further harm in extreme weather situations	**E7B | Adjustment to increased extreme weather conditions** • Improved weather forecast makes it easier for farmers to adopt to the current conditions. e.g. irrigation or protection from hail • New architecture and urban planning due to flooding, hot, dry summers and water shortages.		
E8	**European forest area**	**E8A | Further forest degradation** • More pressure due to yield and harvest • Unsustainable logging and fuel wood harvesting • Impulsive conversion of forests for other land uses like roads and other infrastructure as well as agriculture • Additional degradation due to fires and climate change	**E8B | Stagnating forest degradation** • The global Initiatives from the World Wide Fund For Nature WWF to stop deforestation reached the goal of conservation. • Forest areas still represent a large proportion of the most common type of land cover in Europe and wood is still an important raw material for production • Still degradation due to fires and climate change.	**E8C | Forest conversion to sustainable nature orientated forestry** • Agroforestry is supported by the European Agricultural Fund. Transfer payments are made by the EU to support the reforestation. • Reafforestation is successfully supported by an EU law • Less degradation due to fires, thus considering of local conditions for afforestation, e.g. less share of high productive but more sensitive tree species	
E9	**Agriculture land in the EU**	**E9A | Exacerbated soil degradation due to the agricultural production** • Land use pattern determines the value of economic returns from agriculture and forestry production: The intensification of agrarian land and trying to use the land in the most efficient way results in leaching of soils. • Habitat and land use change still have largest global impact on biodiversity.	**E9B | Use of land for agriculture is still most important** • Further converting of grassland and forestland to agriculture • Agricultural production for food consumption is still one of the predominant land-use activities across the globe and EU	**E9C | Effective use of land is getting more important** • Targeted set-aside of arable land or maintenance of permanent pasture • Overarching land use concepts including food production, conservation of traditional landscapes, biodiversity "production" as well as creating new jobs in rural areas • Spatial planning, which improves local consumption patterns	

E10	**Water supply and regulation in the EU**	**E10A | Increased problems of water scarcity, national regulations** • Significant seasonal fluctuations • Strong water pollution • Increased problems of water scarcity and drought clearly indicate the need for a more sustainable approach to water resource management across Europe.	**E10B | No lack of water supply, national (municipal) water supply** • Improved weather forecast makes it easier for farmers to adopt to the current conditions: There are irrigation systems for artificial rainfall.	**E10C | No lack of water supply, European regulation** • There are new cost saving technologies to turn saltwater into drinkable water and irrigation systems for artificial rainfall. • Denationalization of the local water supply: EU law to international tender for the water supply, which promotes competition within the EU	
E11	**Urbani-zation and land use planning in the EU**	**E11A | Urban sprawl in conflict with agriculture land** • Conflicts in land use: Building on agriculture land and conversion of forests for other land uses like roads and other infrastructure as well as agriculture • Raised soil sealing and land consumption for building	**E11B | Local and national regulations to meet the rural-urban conflicts** • Slightly implementation of measurements to reduce urban sprawl, like the integration of land use and transport planning • Reuse of waste urban land or empty buildings • Changes in national spatial planning laws to handle conflicts in land use • Soil sealing slower than land consumption for building	**E11C | European regulations for integrated rural-urban development** • Spatial planning and regulatory coordination of development, land use change and especially larger projects (changes in European regional planning law to handle conflicts in land use) • Development models for rural-urban regions • Effective mechanisms for cooperation at the level of the rural-urban region, aiming towards joint strategic planning rather than a competition for development • Surface recycling measurements slightly implemented	

E12	**Biodiversity importance in the EU**	**E12A | Measures for biodiversity protection not implemented** - Less implementation of the EU strategies for biodiversity preservation resulting from poor management, inadequate monitoring and enforcement as well as lack of funds - Measures at the national level implemented partially, but in generally there is still belief that the change in biodiversity is harmless in comparison with other environmental problems.	**E12B | Biodiversity protection: Bio-diversity as important as bio-quantity** - Effective and urgent actions are taken at the EU level to halt the loss of biodiversity (Convention on Biological Diversity CBD) - Measures for biodiversity protection implemented according to the targets for 2020 covered by the EU strategy: Tighter controls on Invasive Alien Species and a greater EU contribution to averting global biodiversity loss. - Measures to prevent genetic diversity (intra biodiversity as insurance against habitat damage or species extinction)		
E13	**Fishery policy in the EU**	**E13A | Increased bycatch - No reform of the CFP** - Fast deterioration based on a continuation of the past trend of landings, with no reform 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	**E13B | Partial recovery - Reformed CFP with positive effects** - Partial recovery of the endangered fish stocks due to a reform of the CFP - Strong focus on the security of abundance of marine species (European regulation).	**E13C | End of overfishing - Reformed CFP with positive effects** - Recovery of the endangered fish stocks due to a bold and ambitious reform of the CFP - Realization that fishery in the sea is not just an issue in Europe: There is no local problem of overfishing but an international.	

Table 12: Key factors and future projections of environment scenarios

6.2 Threats Descriptions – Consolidated list of threats

6.2.1 Cyber infrastructure

Title	**Governmental cyber espionage and spying**
Description	**Origin of threat:** manmade, intentional attack **Motives:** The main motive of traditional espionage is to obtaining secrets without the permission of the holder of relevant information. The holder of relevant information can be a person, a company, or governments. Usually spying is done for economic, political or military advantage. Cyber spying typically involves the use of internet to access secrets and other classified information or to control computers or whole networks for a strategic advantage and for psychological, political and physical subversion activities and sabotage. More recently, cyber spying involves analysis of public activity on social networking sites like Facebook and Twitter. Such operations, like non-cyber espionage, are typically illegal in the victim country while fully supported by the highest level of government in the aggressor country. The ethical situation likewise depends on one's viewpoint, particularly one's opinion of the governments involved. In cyber espionage motives are often similar to classical governmental espionage, however methods are very different and often much more sophisticated. **Methods:** The main infrastructure for cyber spying is the Internet. The combination of networks and individual computers is utilized by the use of cracking techniques and malicious software including Trojan horses, root kits, bot nets and a whole range of other preparatory developer and hacking tools. The attack may wholly be perpetrated online from computer desks of professionals on bases in faraway countries or may involve infiltration at home by computer trained conventional spies. **Impact:** Due to the large amount of available digital data and attack frameworks, like metasploit, attacks are usually low resources, high impact attacks. The spying efficiency increased remarkable, with the ongoing improvements in software support.. **Background:** In the last years an increasing number of very large scale cyber attacks, with public backgrounds were discovered. E.g., in March 2009 Ghostnet was discovered, a very large scale cyber spying infrastructure with compromised computers from embassies, foreign ministries and other government offices in 103 countries. The command and control infrastructure was based manly in china. However as almost ever in cyber operations there is no conclusive evidence, that Chinese government was involved. Obviously the purpose of Ghostnet was to develop a long term and large scale spying infrastructure to have this infrastructure available, when necessary. Besides quite a lot of other small scale attacks a cyber attack compromised US military weapons systems in 2013 and an attack to get ASIO (Australian Intelligence Service) blueprints are brought to the media. **Relevance in the future:** In the future it is expected, that cyber espionage capabilities and techniques will improve. It is very likely, that big datasets will be copied by using advanced cyber-attack tools, and that some countries will work on similar hidden attacks like Ghostnet. Therefore there will be a hidden competition between protection capabilities and attack capabilities.
Affected areas	Primarily affected are public institutions military organizations and intelligence services, both in developing defensive and offensive techniques.. However in a second step, all organization, with relevant information for the national security expects infrastructures might be affected.
Affected regions	All countries.
Affected domain	As ICT in high tech countries is critical in almost every domain, all domains with secret information are affected.
Entry period	Ongoing and of increasing importance. Not all countries will do research on offensive capabilities, but almost all will need defensive capabilities
Application period	Since now and open end.
Empirical values	Increasing amount of malware attacks, with public background.
Sources	Weak signals scan, Wikipedia, Yahoo news

Title	**Economic cyber espionage**
Description	**Origin of threat:** manmade, intentional attack **Motives:** Industrial espionage, economic espionage or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security purposes. Economic espionage is conducted or orchestrated by governments and is international in scope, while traditional industrial or corporate espionage occurs between companies or corporations. The main intention of economic cyber espionage with e.g. IPR theft, or business secret intelligence, remains the same, in comparison to traditional economic espionage, but cyber espionage makes full use of all new digital surveillance methods, often in combination with new methods of the national intelligence infrastructure. **Vulnerabilities/Methods:** In economic cyber espionage, the attacker make use of cracking techniques and malicious software including trojan horses, root kits, bot nets and a whole range of other preparatory developer and hacking tools. Frameworks like metasploit, the Elderwood framework and other are used to collect secret information from the target. Main targets are usually high technology industries, like ICT, biotechnology, aerospace, telecommunications, transportation and engine technology, automobiles, machine tools, energy, materials and other. If the economic espionage is supported by national administration unites, methods from private hacker are combined with modern public intelligence methods like telecommunication interception. **Impact:** Main impact is the loss of intellectual properties, national competitive advantages in industries and economic disadvantages of all kinds. **Background:** In the last years, an increasing amount of cyber espionage was reported from different medias. E.g. on January 13, 2010, Google Inc. announced that operators, from within China, had hacked into their Google China operation, stealing intellectual property and, in particular, accessing the email accounts of human rights activists. Usually these threats are considered as advanced persistent threat (APT) which means, they refer to a capability and the intent to persistently and effectively target a specific entity, often the main competitor or high tech owners with the full power of national intelligence infrastructure, including satellite surveillance, full access to all telecommunication networks and much more., . **Relevance in the future:** In the future it is expected, that economic cyber espionage capabilities and techniques will improve. It is very likely, that there will be a hidden competition between protection capabilities and attack capabilities. Recent events point to the direction, that there will be an increasing number of countries with public support for it.
Affected areas	The ordinary IPR owner is addressed by this threat.
Affected regions	All countries.
Affected domain	As ICT in high tech countries is critical in almost every domain, all domains with secret information are affected.
Entry period	Ongoing and of increasing importance. Not all countries will do research on offensive capabilities, but almost all will need defensive capabilities
Application period	Since now and open end.
Empirical values	Increasing amount of malware attacks.
Sources	Weak signal scan, Wikipedia, Symantec White paper The Elderwood Project

Title	**Cyber warfare**
Description	**Origin of threat:** manmade, intentional attack **Motives:** In 2010, the Economist described cyberspace as the fifth domain of warfare, in addition to the traditional domains: land, sea, air, and space. The future will show, whether this is true or not. However in reference to different escalation phases, cyber war activities starts at a very early stage and will be part of all escalation phases, with different motivation in every stage. In early stages, the main motivation is often reconnaissance, misinformation, espionage and preparation. Later deception, sabotage, DoS attack and destruction of critical infrastructure are additional motivations. **Methods:** In reference to specific motivations, there are hundreds of different methods used, in cyber warfare actions, usually in combination. Methods for legal and not legal reconnaissance includes tools for information gathering, e.g. whois, DNS, password decryption, etc, scanning tools, like Nessus and nmap. Missinformation and preparation is done with integrated attack frameworks, like metasploit, remote administration tools, like

	trojans and obfuscation tools like log manipulation, vpn and onion routing networks. Sabotage is done with trojans, worms and viruses. Supporting methods are almost all programming support software, like disassembler, debugger, ide and many other. **Impact:** Break of data secrecy, lost of trust in governmental data, lost of ICT services, damage of critical infrastructure. Attacks are usually low resources, high impact attacks. **Background:** In the past years, an increasing number of governmental cyber attack cases have become public. In Estonia 2007, a remarkable number of public websites where closed down. The Irak was attacked, by stucks net and an unknown number of diplomatic services and other targets where attacked by ghost net. These are probable precursors of future cyber attacks. A large number of nations introduce a new cyber security strategy, while spending an increasing amount of money to build up cyber warfare capabilities. One of the hardest issues in cyber counterintelligence is the problem of "Attribution". Unlike conventional warfare, figuring out who is behind an attack can be very difficult. **Relevance in the future:** In the future it is expected, that nations will try to extend their national competitive advantages in cyber security. Public unknown zero day exploits are very important for the competitive advantage in cyber attacks. Therefore it is a strong precursor for future developments in cyber warfare that prices for zero day exploits increased dramatically, on the black marked. In line with general trends to network centric warfare and the increasing importance of drones and robots, cyber warfare will have a wide range of possible applications in the near future.
Affected areas	Primarily affected are public institutions. However in a second step, all critical infrastructures might be affected.
Affected regions	All high tech countries are in risk for a cyber warfare attack. This attack is suitable for asymmetric warfare.
Affected domain	As ICT in high tech countries is critical in almost every domain, all domains are affected.
Entry period	There is an increasing probability, that cyber warfare actions will extend the portfolio of governmental reactions on unfriendly behavior of other nations. There is no precursor for a trend brake visible.
Application period	Since now and open end.
Empirical values	Exponential growth in malware attacks, as reported from private cyber security companies is a precursor for this threat. Countries donate an increasing amount of money in the last years, to build up cyber warfare capabilities. Cases, like stuxnet, ghost net, Gregorian cyber attack and the China cyber security strategy are strong precursor in favor of future cyber warfare.
Sources	Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners By Jason Andress, Steve Winterfeld

Title	**Data leak, - loss, and - trading events - black markets for information**
Description	**Origin of threat:** accidental event or intentional attack **Motives:** In line with the increasing digitalization of .text-, sound-, picture-, and video data, there will be more and more data repositories with very large amounts of private and secret data in the future. In the last years, the trend in data loss events points to the fact that data sets can get lost, even if they are very large and well protected. In line, with outsourcing efforts and cloud services, it can be expected that the number of data leak and - loss events increase with the number of valuable data sets. An additional risk is that leaked or lost information is not destroyed and enters in some ways enter the black market (lost notebooks, lost usb sticks etc.), where it often gets combined with already existing other datasets. That points to a trend of commercializing which is expected to be one of the most important motives in the future in dealing with data sets. Specific for leaked datasets, political and intrinsic motivation might be even more important. **Methods:** Most data loss events are accidental and not intentional. Thus no specific method applies. However for leaked information and black markets with high value data sets this is different. In this case, cloud computing attacks, bot-nets, phishing or pharming contribute to additional procurement of valuable information. Leaked information in particular is exchanged in anonymous encrypted networks, like free net or tor. Whistleblower platforms, like Wiki leaks are used to initially make leaks very comfortable and secure. In black markets, like silk road, is often an incentive to improve available datasets with intentional acquisition of new corresponding data sets, to increase the economic rewards. **Impact:** In the long run, breaks of data secrecy will lead to a lost of trust in ICT

infrastructure, for the one, who are working with this. On the other hand, open information and transparency can increase trust, if the leaked information are concise to the open public information. For ICT services, data lost and data leaks events can lead to damages of critical infrastructure, but reacting on this can lead to a more resilient ICT infrastructure. These ambivalent impacts shows, that the overall consequences depends probably much on future strategic decision and behavior of the data owner.

Background: In the last years, a number of whistle blowing platforms (e.g. wikileaks, openleaks) and peer to peer networks (freenet, I2P, RShare/ StealthNet, MUTE, BitTorrent) where set up, to support anonymous data leaks and secure exchange of all sorts of data, often from illegal sources. Besides copy right infringements on peer to peer networks, there is an increasing probability of having large illegal datasets, shared on anonymous peer to peer networks and traded on the black markets, like silk road.

Relevance in the future: In the future it can be expected, that even larger and more important datasets are leaked occasionally. Large credit card datasets, with data about more than 40 Mio credit card owner, have already been leaked. The general public will probably get access to secret governmental information, for a while and then it will probably get more and more difficult to judge, whether the leaked or lost information is real. The public administration will get detailed information from industries and industries will get private information from their customers. Pressure groups, like anonymous will take advantage from the public awareness of data misuse.

Affected areas	Primarily affected are all institutions with large valuable data sets.
Affected regions	All countries.
Affected domain	Cyber infrastructure
Entry period	There is an increasing probability, that large scale events will take place.
Application period	Since now and open end.
Empirical values	Number of data leak and data loss events, black market dynamics.
Sources	datalossdb.org, Wikipedia, Weak Signal scan

Title	**Unexpected results from large scale data fusion**
Description	**Origin of threat:** manmade, intentional attack or unintentional result
	Motives: Data fusion in itself is not a threat. It is simply the process of integration of multiple data sources and knowledge representing the same real-world object into a consistent, accurate, and useful representation. However services, like search engines, voice interfaces for cell phones, picture search engines and other services, with databases in behind, generate a potential for misuse. Motives for misuse are economic reward, political corruption and power or unmindful software development.
	Methods: Data fusion processes are often categorized as low, intermediate or high, depending on the processing stage at which fusion takes place. Low level data fusion combines several sources of raw data to produce new raw data. The expectation is that fused data is more informative and synthetic than the original inputs. For example, sensor fusion is also known as (multi-sensor) data fusion and is a subset of information fusion. Intermediate or high level data fusion uses analytical results to generate new knowledge, often used in decision support.
	Impact:
	Background: In the past years, there is an increasing amount of services available, which build upon, or make use of very large data sets with private data. Search engines like Google, Yahoo and other were one of the first services with such large and powerful datasets, with private data on a global level. A Yahoo search request dataset was leaked, some years ago. From this dataset, it was obvious, that it is possible, to identify e.g. military staff, with pedophile sexual orientation. Leaked knowledge about this, would expose the user as target for extortion and espionage. Other datasets are, e.g. the language pattern of speech recognition from Apple and Android, picture search engines voice and video from Google glasses, internet log data, .web mail services and so on.
	Relevance in the future: A typical data fusion threat would arise if e.g. a robot with artificial intelligence, like Samsung SGR-A1 is used in boarder protection, as one part of the threat. In addition the speech recognition would have been trained with the language pattern from 5 billion smart phone user from Apple (with Siri) and Android, with the corresponding application. This would give SGR-A1 the capability to identify all smart phone users. However, even if this is a not very likely future scenario, other datasets might be useful for challenging services or for future surveillance technologies.
Affected areas	Primarily affected are citizens, on a global level.

Affected regions	This threat is more relevant in nations with authoritarian governments or dictatorship, as well as corrupt data service provider on a global level.
Affected domain	all domains are affected, but based on misuse of ICT.
Entry period	near future
Application period	Since near future and open end.
Empirical values	Large data sets, with private data
Sources	A General Data Fusion Architecture, Hervaldo S. Carvalho, Center For Future Health, University of Rochester, Rochester, NY, U.S.A, Information and Intelligence Fusion Centers edited by Todd Masse, Siobhan O'Neil

Title	**Insider attacks**
Description	**Origin of threat:** manmade **Motives:** • A negative work-related event triggered most insiders' actions or the former employees or contractors had to leave involuntarily their position. • To attack some aspect of an organization or direct specific harm toward an individual(s), most likely as revenge. • Attacks can result in data theft/leakage/ trading, destroy of virtual or physical goods etc. **Methods/Vulnerabilities:** Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed. This sophisticated attack tools included a script or program; an autonomous agent; toolkits; flooding; probing; scanning; spoofing The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks. Remote access was used to carry out the majority of the attacks. Often a lack of internal security standards ease the attacks **Impacts:** Insider activities caused organizations financial losses, negative impacts to their business operations and damage to their reputation. Though the number of attacks is lower, the damage is in most cases dramatically higher due to the fact that insiders are in a better "attack" position. **Background:** Insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases. Most of the insiders who committed acts of sabotage were former employees who had held a technical position with the targeted organizations or contractors of the affected organizations, but also current employees or contractors. **Future importance:** it is likely that with the increased diffusion of ICT more and more internal security problems are created. This raises the potentials of successful insider attacks.
Affected areas	The majority of the incidents of insider sabotage were perpetrated against private sector organizations. There were barely government entities, but the public ones are the most known cases. The incidents affected organizations in the following sectors, e.g. banking and finance; continuity of government; defense industrial base; food; information and telecommunications; postal and shipping; public health. Most incidents happened in the information and telecommunications sector.
Affected regions	In principle all regions
Affected domain	Cyber infrastructure.
Entry period	now
Application period	
Empirical values	Efforts to estimate how often companies face attacks from within are difficult to make. It has been suggested that insider attacks are under-reported to law enforcement and prosecutors. Reasons for such under-reporting include an insufficient level of damage to warrant prosecution, a lack of evidence or insufficient information to prosecute, and concerns about negative publicity. Also insider attacks in public services are seldom reported, only some cases (Manning e.g.) showed the potential of these kind of attacks.
Source	DARPA

Title	**Cyber extortion (economical)**
Description	**Origin of threat:** manmade **Motives:** manumission payment (financial, criminal) **Vulnerabilities/Methods:** extortions are based on • computer hijacking through Trojans or other remote control software exploiting known or unknown software flaws of a system • data theft based illegal access exploiting known or unknown software flaws of a system **Impacts:** loss of money and trust **Background:** at the moment there are two ways of cyber extortion: 1) Trojans are used to block computable devices indicating that illegal content (software, multimedia, child pornography etc.) is found. Removing this block requires a payment to an unknown bank account; 2) access is used for threats related to publish sensitive material. While the first mainly affects normal user, the latter one exist mainly in business, particular for companies with strong internet based transactions (online retailer etc.) The **future importance** of this threat is based on the growing interconnection of computable devices and infrastructures, which for example could enable extortion of companies based on the blockade of critical production systems. Already today the use private USB sticks open possibilities also to attack "closed" systems, but recent trends like "Bring your own device" (BYOD) will increase the problem even more. Reason is that private devices are often less protected and the integration of such devices in a company network creates many possible new vectors for attack.
Affected areas	Primarily affected are consumers and companies, maybe also public institutions. It is therefore relevant to all kind of institutions and natural persons. It can disturb the daily operations of industries including banking etc. and influencing daily life. Highest risk is that damage to the physical system as well as loss of trust by consumers will occur and impact company negative.
Affected regions	In principle it is relevant for all medium and high developed countries that are heavenly relying on IT based production systems and services. But also countries with little number of such systems can be affected, in particular if the economy is strongly relying on it. The threat might lead to company breakdowns, massive loss of trust or even economic crisis.
Affected domain	In principle extortion is could be used in all domains, but in cyber infrastructure the probability is the highest due to easy implementation, low risk of attribution etc.
Ethics	Monetary damage, psychological harm
Entry period	It already appeared in some forms like for example consumer attacks. There are also cases of extortion of companies known, but no clarity about level of threat and success.
Application period	It already exists, but will increase in the future. In particular targets and methods will change.
Empirical values	There are many cases known either of blocking malware or attempts to extort companies, but there is no aggregated statistic on it. Drivers are as indicated trends like internet of things and services and consumerization of IT (BYOD).
Source	ITU

Title	**Governmental sabotage**
Description	**Origin of threat:** manmade, intentional **Motives**: achieving political/security aims **Methods/ vulnerabilites:** manipulation of specific targeted systems of the enemy: • Illegal access to a system from outside exploiting software flaws • Illegal access from outside through social engineering (f.e. spread of USB sticks) • Illegal access through insider job **Impacts:** harm (physical or digital) systems of potential enemy and reducing its capabilities to achieve specific goals or reduce its capacity for defense **Background:** the growing digitalization of all processes, in particular also in security relevant areas like military R&D and systems, lead to an increased risk of targeted attacks against specific systems. In particular such attacks could be used to cover other operations as well as to influence the general capacities. Both cases already took place in the last years, for example in Iran or Syria.

	Future importance: though this type of attacks is very dark grey zone close to cyber warfare it seems very likely that it will gain of importance in the next years. In particular due to the problems of attribution of attacks and its specific character it offers a bypass to achieve political or military aims without crossing the border to official act of aggression.
Affected areas	Targets are potentially all types of public or private intuitions, which have relevance for specific very important processes in research or military etc. The highest risk is potential loss of capabilities to defend or secure important institutions or programs with a high value for a nation.
Affected regions	All countries, but in particular in highly developed as well as emerging countries due to the required level of digitalization.
Affected domain	Cyber
Ethics	Cause of collateral damage (loss or damage of people)
Entry period	in the next years
Application period	It exist already and will continue
Empirical values	There is no official statistics, but some cases are well known like the attempts to damage the Iranian atom program as well as the case of Syrian radar control defects in the case of Israelian attacks.
Source	diverse

Title	**Terroristic sabotage (Government and critical infrastructure)**
Description	**Origin of threat:** manmade **Motives:** • Shocking actions of terrorists to demonstrate their power and capability to challenge their enemies. • Violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda. • Intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives. • Some examinations of cyber-terrorism focus on the physical destruction of information hardware and software, or physical damage to personnel or equipment using information technology as the medium. • Political motive for their activities. **Methods/Vulnerabilities:** Attacks of this sort requires that messages and computer commands are transmitted, programs and malicious software be emplaced, fraudulent transactions take place, and information be available for exploitation. Defacing websites, crashing portions of a target network, accessing enemy information, denying network access to other groups, manipulating financial confidence and causing panic exemplify this type of attack. The goal of computer sabotage is to hinder the normal functioning of a computer or computer system. It can include: changing data; deleting data; destroying data or programs with logic bombs; crashing systems; holding data hostage; destroying hardware or facilities; entering data incorrectly, exposing sensitive and embarrassing proprietary data to public view such as the salaries of top executives. They can plant viruses, Trojan horses or worms, browse through file systems or program malicious code with little chance of detection and with almost total impunity. **Impacts:** Terroristic sabotage investigations can be conducted for a wide range of actions, from a harmful and libelous social networking post, all the way up to the hacking and leaking of corporate consumer information such as credit card numbers or industry secrets. Computers control nearly every aspect of our lives: the operation of cars, the flow of data in business, and most importantly, the services vital to economic growth and national security. Potential targets in internet sabotage include all aspects of the Internet, from the backbones of the Web to the Internet Service Providers, to the varying types of data communication mediums and network equipment of companies and individuals. Most vulnerable are enterprise information systems and databases. **Background:** The Cyber Division of the FBI states that in the future, cyber-terrorism may become a viable option to traditional physical acts of violence due to: Anonymity; Diverse targets; Low risk of detection; Low risk of personal injury; Low investment; Operate from nearly any location. **Future Importance:** The next generation of terrorists will grow up in a digital world, with

	ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber-terrorism than the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Hackers and insiders might be recruited by terrorists or become self-recruiting cyber-terrorists. Cell phones are a likely to become a bigger target for cyber sabotage in the future as they are used more and more for financial transactions, information and purchasing, and are heavily used for workplace functions. The increased popularity of tablets will make them a bigger target in the near future they are more easily hacked than regular computers.
Affected areas	In particular critical Infrastructures connected via networks are potential targets of cyber terrorists. These infrastructures make extensive use of computer hardware, software, and communications systems. It includes Energy systems; Emergency services; Telecommunication; Banking and finance; Transportation; Water systemIf unauthorized personnel gain cyber access to these systems, any alterations to settings or data can have disastrous consequences, resulting in widespread blackouts or other failures. Furthermore national security systems, which more and more depends heavily on advanced computers.
Affected regions	All regions, primarily North America and Western Europe.
Affected domain	Cyber
Entry period	Now to near future
Application period	No end
Empirical values	Increasing number of political motivated campaigns against specific countries etc.
Source	http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA439217 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/the-english-version-of-the-cyber-security-report-2012.html http://www.britannica.com/EBchecked/topic/130595/cybercrime/235711/Sabotage?anchor=ref829246 http://www.icsworld.com/Private_Investigation_Case_Types/Cyber_Sabotage_Investigations.aspx http://defensetech.org/2008/02/06/cyber-sabotage/ https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/the-english-version-of-the-cyber-security-report-2012.html http://www.mintaka.com/whitepaper/White%20Paper%20-%20Security.pdf http://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf http://www.cjimagazine.com/archives/cji4411.html?id=37 http://ascentlookout.atos.net/en-us/sep_trends/economic/cyber_threat/default.htm

Title	**Commercial desinformation**
Description	**Origin of threat:** manmade **Motives**: financial gain **Vulnerabilities/Methods:** manipulation of digital information on different ways: ● Illegal access to a system from outside exploiting software flaws ● Illegal access from outside through social engineering ● Illegal access through insider job **Impacts:** damage the reputation of a company in different ways leading to loss of competition/contracts or manipulation stock markets etc. **Background:** the growing digitalization of business processes offers the possibility to use false information on companies either to harm the company directly by damaging their competitiveness in different was (wrong information, misleading information on contracts) or to misuse information on companies for illegal transactions (insider deals). **Future importance:** due to the growing digitalization as well as the fact that sensitive information are transferred through data centers (cloud computing), the risk of such disinformation and manipulation will strongly increase
Affected areas	Targets are potentially all types of companies ranging from industry to services, in particular ones either with a highly competitive markets as well as listed companies. Beside the companies concerned the crime prosecution forces as well as other public institutions dealing with competition are concerned. The highest risk is potential damages for the companies, but also for contractors as well as other stock exchange participants. Moreover it could result in distrust and collapse of

	single firms affecting people employed and the social security systems.
Affected regions	Most likely this will happen in highly developed as well as emerging countries due to the required level of digitalization. Since it is limited to single companies the effect might be only a economical damage, but on the long turn a series of such events could influence the public trust in economical system, which is the biggest threat.
Affected domain	Only relevant for cyber
Ethics	Economical harm, violation of privacy may included
Entry period	in the next years
Application period	It exist already and will continue
Empirical values	At the moment there are no empirical values existing
Source	ITU

Title	**Political desinformation**
Description	**Origin of threat:** manmade **Motives**: achieving political aims **Methods/ vulnerabilites:** manipulation of digital information on different ways: • Illegal access to a system from outside exploiting software flaws • Illegal access from outside through social engineering • Illegal access through insider job **Impacts:** influencing the public view on political opponents in different ways leading to loss of trust, public support or similar **Background:** the growing digitalization of governmental processes offers the possibility to use false information on public institutions either to harm the institution directly, in particular to influence public opinion. **Future importance:** due to the growing digitalization as well as the fact that sensitive information are transferred through data centers (cloud computing), the risk of such disinformation and manipulation will strongly increase
Affected areas	Targets are potentially all types of public intuitions, in particular governments, political parties etc. The highest risk is potential loss of reputation and trust. Moreover it could result in distrust to public and political system.
Affected regions	All countries, but in particular in highly developed as well as emerging countries due to the required level of digitalization. In the long run a series of such events could influence the public trust in political system, which is the biggest threat.
Affected domain	Cyber
Ethics	Reputational damage, violation of privacy may included
Entry period	in the next years
Application period	It exist already and will continue
Empirical values	At the moment there are no empirical values existing
Source	Wired

Title	**Digital vigilantism**
Description	**Origin of threat:** manmade **Motives:** "Vigilante justice" is rationalized by the idea that adequate legal mechanisms for criminal punishment are either nonexistent or insufficient. Vigilantes typically see government as ineffective in enforcing the law; and such individuals often presume to justify their actions as fulfillment of the wishes of "the community". **Methods:** The different types of Internet vigilantism are debatable. There is no single source which states what is and what isn't Internet vigilante behavior. This phenomenon is studied on a case-to-case basis. A desktop research produced the following events. • Scam baiting • Identity theft activism • Cyber/public shaming • Counter-terrorism • Anti-pedophilia activism **Impacts:** Vigilante behavior involves various degrees of violence. Vigilantes may assault targets verbally or physically.

	Cyber vigilantism damages significantly the real life of victims. E.g. they had to leave their hometown. **Background:** In the 1990s, cyber-vigilantism emerged where so-called "ethical" or "white hat" hackers go after sexual predators, terrorists, spammers, auction frauds, and copyright infringers on the Internet. For example, some activist groups are involved in anti-terrorism, and other activist groups pose as "honeypot" targets for child molesters. The most well-known examples are Anonymous, the online international organization for taking actions regarding protests, and public shaming which is to bring disgrace on people who do anti-social behaviors against what general society believes as justice, by publicizing their personal information online. **Future Importance:** Online vigilantism is on the rise because the so-called vigilantes can maintain the anonymity that keeps them safe from the repercussions of their actions.
Affected areas	Particularly, online social networking tools have made dissemination of information on the Internet very easy and this leads to serious personal damages.
Affected regions	Internet vigilante justice occurs worldwide. Public shaming is a more intensified form than the early type of Anonymous by focusing on making targeted people whose behavior was socially irresponsible and immoral embarrassed not only locally but also internationally. It is more frequently found in Asia than in western countries, because it relates Asian values and norms that place emphasis on social responsibility and politeness inside groups. China has a very special tool for the effective accomplishment of public shaming; Human Flesh Search Engine. It is the network made up of massive Chinese internet users to identify and release information on a particular individual or group who deserve blame for acting immorally. Users who contribute to the search engine aim to achieve online vigilante justice by their own hands, punishing people who provoke an outburst of the public anger.
Affected domain	Cyber infrastructure.
Entry period	
Application period	
Empirical values	Calls for action out of the sample size 1/10 of all posts equate to 249 total posts. Of those posts 60% did not have a "call to action" (negative), which leaves 40% (positive) to have called for action. Those that made a call for action then either supported vigilante justice or did not. Those that made a call for action nearly 90% (support) involved were supportive of vigilante justice. While only 10% (action against) were against those that called for vigilante justice. Punishment-based results occurred more often and had the highest number of occurrences. Threat occurred seventeen total times for 19% of the time. Aversive stimulation occurred eleven times accounting for 12%. Negative esteem occurred fourteen times and was 16% of total occurrences. Negative moral occurred twenty-eight times and accounted for 31%. Ultimatum occurred only once and 1% of total occurrences. Warning had nineteen total occurrences, accounting for 21%.
Source	Brenner, S. Is There Such a Thing as 'Virtual Crime'? California Criminal Law Review. [Online, 2001.] California Criminal Law Review Website. http://www.boalt.org/ CCLR/v4/v4brenner.htm; Schell, B.H. and Martin, C. 2004. Contemporary World Issues Series: Cybercrime: A Reference Handbook. Santa Barbara, CA: ABC-CLIO. http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2561&context=etd http://en.wikipedia.org/wiki/Internet_vigilantism http://www.drtomoconnor.com/3100/3100lect04a.htm http://brianrowe.org/LIS550/2012/03/14/internet-vigilantism-anonymous-and-public-shaming/ http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2561&context=etd

Title	**Cyber bullying / reputational damage**
Description	**Origin of threat:** manmade **Motives:** Harassment, humiliation, ridicule, … **Methods:** • Forwarding private messages, pictures, or videos and therefore, compromising the privacy of the victim. • Assuming a false identity on social networking sites in order to persistently harass others.

	• Sending cruel or harassing emails or text messages that could be humiliating, threatening, or both. • Posting hurtful or embarrassing posts on Facebook or any other social networking site (Twitter, Myspace, Formspring, Instagram, Snapchat, etc…). • Name-calling over the Internet. • Circulating sexually suggestive images to devalue a person's existence and/or to humiliate him/her. • Mean, hurtful comments and spreading rumors are the most common type of cyber bullying. **Impacts:** Cyber bullying can present very real dangers, ranging from low self-esteem to suicide. It also has an impact on privacy issues. **Background:** There are different levels of cyber bullying: In some cases, a person or people are ignorant and do not know what the consequences of their actions could entail. In other situations though, people can be deliberately threatening and menacing, even putting the life of another in danger. **Future Importance:**"Slut-shaming," is a disturbing trend in which teens harshly criticize each other's body types and style (Article: nydailynews.com, Jan. 2013)
Affected areas	Cyberbullying affects mainly teenager, but also adults. Most of the teens use a cell phone regularly, making it the most popular form of technology and a common medium for cyber bullying.
Affected regions	This threat is relevant all around the world (see Empirical values).
Affected domain	Cyber
Entry period	now
Application period	No end
Empirical values	General Statistics on Cyber Bullying: • **Over 95%** of teenagers use social networking sites to communicate with peers. • **Over 25%** of teens have been bullied repeatedly through text messages or the Internet. • **90%** of victims will not inform a parent or trusted adult of their abuse. • **1 in 3** teens have experienced cyber-threats online. • **85%** of teenage online users have been cyber bullied at least once • **87%** of teens use cell phones, over **93%** of teens are online, and **75%** of teens use Facebook alone (Cyberbullying Research Center, https://www.ncjrs.gov/internetsafety/cyber.html) • Belgium: 34.3% of Belgian teenagers have been bullied through the Internet or cellular devices (European Commission Survey, Nov. 2009.) • Poland: 52% of Polish Internet users aged 12-17 have been exposed to abuse on the Web or via mobile phones (European Commission Survey, Nov. 2009.) • Germany: 14.1% of students also experience the kinds of incidents (harassment, denigration, outing & trickery and exclusion) that constitute cyberbullying (Cyberbullying in Germany, Psychology Science Quarterly, 2009.) • Japan: Ten percent of high school students said they have been harassed through e-mails, websites or blogs (Survey by the Hyogo Prefectual Board of Education, 2007 (Citied in Reuters article).) • Spain: Between 25% and 29% of all teenagers have been bullied via their mobile phone or the internet over the past year. (University of Valencia (UV), 2010.) • South Korea: A survey of 272 students at four South Korean universities found that three-fourths knew a victim of cyber bullying and more than half knew a cyberbully. (University of South Florida, 2010)
Source	http://cyberbullyingstatistics.org, https://www.ncjrs.gov/internetsafety/cyber.html, http://www.endcyberbullying.org Cyberbullying Research Center www.nydailynews.com European Commission Survey, Nov. 2009 Psychology Science Quarterly, 2009 Survey by the Hyogo Prefectual Board of Education, 2007 University of Valencia (UV), 2010 University of South Florida, 2010

Title	**Network breakdown – accidental**
Description	**Origin of threat:** by accident **Motives:** no motive **Vulnerabilities/Methods:** accidental network breakdown can happen • if a routine software update turns out to destabilize the system • if manual changes to system destabilize the system • if central switch/cable is destroyed by accident **Impacts:** breakdown of internet connectivity and cascading effects **Background:** due to the fact that the current internet architecture is based on an open approach several possibilities that could lead to a network breakdown. One example for vulnerabilities is the Domain Name System (DNS), but there are other systems affected. Failures of it either caused by software or hardware can lead to breakdown of the internet connectivity. Another threat can be caused by accidental damage to physical components like main connecting cables or central switches. Examples in the past occur because of shipping or construction works. F**uture importance:** since the basic architecture will not change, but many new functionalities are enabled the possibilities of errors and mistakes will increase. Additionally it is also not probable that physical redundancy in case of critical components like sea cables will be installed due to financial motives.
Affected areas	Due to the basic function of the network, a failure would affect all people. Nevertheless it is most relevant for the different CERT and national or regional nodes. It will affect society and economy through a slow down or stop of connectivity at all, which will influence many daily operations for consumers as well as for companies. Most dangerous is that based on a breakdown of the network cascading effects can occur like breakdown of other infrastructure systems due to their growing interrelation with the network (for example smart grids).
Affected regions	In principle such a breakdown could affect individual regions up to the whole world, depended on what system or hardware is affected. Examples are the cut-off internet sea cable affecting Australia as well as problems within different root zones of the DNS system.
Affected domain	It is only relevant within the cyber infrastructure domain
Ethics	none
Entry period	Incidents with regional impact occurred already, but no global one until now.
Application period	It is already relevant and will stay as long as there are no ground lying efforts to change architecture of the internet
Empirical values	Few estimations on the costs of Internet breakdown exist (see OECD), but the reliability is open Drivers are: growing complexity in an old architecture; poor implementation of redundancy for economical reason
Source	ENISA

Title	**Network breakdown - natural**
Description	**Origin of threat:** natural disaster **Motives:** no motive **Vulnerabilities/Methods:** network breakdown based on natural catastrophe, mostly related to physical damage to network infrastructure **Impacts:** slowdown/breakdown of internet connectivity and cascading effects **Background:** as already shown by natural disasters like the recently the storm Sandy, such events can heavenly influence the connectivity of the communication networks. Most likely is that a natural disaster like storm or earthquakes will damage the physical infrastructure and lead to a slow down or breakdown of the network. Moreover cascading effects could occur because of the interrelation of different infrastructure systems and the possibility that they amplifying each other. **Future importance:** given the fact that the number of natural disaster increased in the last periods and that particular highly developed countries rely more and more on infrastructure services, the threat will gain of importance. In particular cascading effects will gain of importance due to the growing interrelation of infrastructure systems.
Affected areas	Due to the basic function of the network, a failure would affect all people. Nevertheless it

	is mot relevant for the different CERT and national or regional nodes. It will affect society and economy through a slow down or stop of connectivity at all, which will influence many daily operations for consumers as well as for companies. Most dangerous is that based on a breakdown of the network cascading effects can occur like breakdown of other infrastructure systems.
Affected regions	Due to the regional character of natural disasters mainly regions would be affected. Nevertheless there is a risk that it hits specific regions with high importance so that could at least lead to impacts in the wider area or some effects on global level. Another point is that cascading effects on other infrastructure systems could have the same consequences and impacts.
Affected domain	It is only relevant within the cyber infrastructure domain
Ethics	none
Entry period	Incidents with regional impact occurred already, but no global one until now.
Application period	It is already relevant and will stay
Empirical values	There are no empirical values of the total costs of single events like Sandy. Even in the calculations of reinsurance companies this effects does not play a role at the moment (no insurance cover it)
Source	ENISA

Title	**Thievery – burglary**
Description	**Origin of threat:** manmade, intentional **Motives**: economic/financial gains **Methods/ vulnerabilites:** thievery, fraud and burglary appear in different forms as one of the main fields of activity of cyber criminals. Overall the motive is to misuse inexperienced or careless consumer to gain access or to their financial details or to convince them to give money. Some recent forms are: • Identity theft – misuse of personal data to create accounts for example credit cards etc. in order to exploit them • Different types of fraud like for example the "Nigeria connection" • Misuse of financial data (credit card information) to order goods In future also other types of attacks or vulnerabilities are possible One example is "digital pocket picking" for smart phones which are used as wallets (i.e. NFC based payments). Overall the attacks are ased on the illegal access of data, in particular either company data or direct from the consumer (phishing), the misuse of trust of inexperienced user in combination with social engineering techniques or illegal access to systems. A more new form seems to be digital variants of institutional attacks like digital bank robbery exploiting weak spots of business IT. More well known are different types of fraud attempts in casino or similar **Impacts:** Financial loss for individuals or in some cases institutions. In the latter case in particular the loss of reputation will be in the long run very harmful. **Background:** the growing digitalization of all processes in everyday life will increase the possibilities to perform such attacks Moreover the growing differences between very advanced and multiple services and a lack of awareness, in particular on the consumer side, enable this type of attacks. **Future importance:** While many examples of these type are already well known and for example credit card companies apply more and more advanced fraud detection systems (based for example on big data), the risk of becoming will not decrease because of growing number of attacks as well as of more and more developing attack technology that always uses the newest exploits. Overall the importance of these activities will grow, though it will be hard to forecast which specific types will appear or loose of importance.
Affected areas	Targets are foremost consumers, which are caught by software exploits, phishing attacks or similar. But also intuitions like banks could become more and more target of such efforts. While it is mostly an individual risk, the growing number could lead to effect that people's distrust in digital systems will decrease. In the long rung this could influence the development of the overall economy negatively.
Affected regions	All countries, but in particular in highly developed as well as emerging countries due to the required level of digitalization.
Affected domain	Cyber
Ethics	Violation of privacy

Entry period	in the next years
Application period	It exist already and will continue
Empirical values	There is no official statistics, but some cases are well known like the attempts to damage the Iranian atom program as well as the case of Syrian radar control defects in the case of Israeli attacks.
Source	diverse

6.2.2 Nuclear

Title	**Nuclear power plant accident**
Description	**Origin of threat:** manmade, natural hazard or technical failure **Motives:** no motives **Methods:** • Loss of coolant A loss-of-coolant accident (LOCA) is a mode of failure for a nuclear reactor; if not managed effectively, the results of a LOCA could result in reactor core damage.[1] • Criticality accident A criticality accident is an uncontrolled nuclear chain reaction. It represents the unintentional assembly of a critical mass of a given fissile material, such as enriched uranium or plutonium, in an unprotected environment. The assembly of a critical mass establishes a nuclear chain reaction. The resulting radiation contains both a neutron and gamma ray component and is extremely dangerous to unprotected humans nearby.[2] • Decay heat accident Decay heat is the heat released as a result of radioactive decay. In nuclear reactor engineering, decay heat plays an important role in reactor heat generation during the relatively short time after the reactor has been shut down and nuclear chain reactions have been suspended. Failure to remove decay heat may cause the reactor core temperature to rise to dangerous levels and has caused nuclear accidents.[3],[4] • Human error An assessment conducted by the Commissariat à l'Énergie Atomique (CEA) in France concluded that no amount of technical innovation can eliminate the risk of human-induced errors associated with the operation of nuclear power plants. Two types of mistakes were deemed most serious: errors committed during field operations, such as maintenance and testing, that can cause an accident; and human errors made during small accidents that cascade to complete failure.[5] **Impacts:** The international nuclear and radiological event scale (INES) classifies nuclear and radiological accidents and incidents on a scale of 1 to 7: Levels 1–3 are called incidents" and Levels 4–7 "accidents". The scale is designed so that the severity of an event is about ten times greater for each increase in level on the scale. [6] The Fukushima Daiichi nuclear disaster is only the second disaster (along with Chernobyl) to measure Level 7 on the International Nuclear Event Scale.[7] **Background:** The prime example of a mayor nuclear accident is one in which a reactor core is damaged and significant amounts of radioactivity are released.[5] It was reported that worldwide there have been 99 accidents at nuclear power plants.[5] Serious nuclear power plant accidents include the Fukushima Daiichi nuclear disaster (2011), Chernobyl disaster (1986), Three Mile Island accident (1979), and the SL-1 accident (1961).[8] **Future Importance:** Some European countries announced plans to move away from nuclear power. But, globally, nuclear power looks set to continue to grow steadily, although more slowly than it was expected before the Fukushima Daiichi accident. There are 437 operating nuclear power reactors in the world today. The latest IAEA projections suggest that the number could increase by 80 or 90 in the next 20 years. It could even double. At the moment, there are 66 new reactors under construction. Seven of them are in India. Other major users of nuclear power such as China and Russia also have significant expansion plans. The United Arab Emirates has started building a nuclear power plant. A number of other

	countries have also taken the decision to introduce nuclear power, including Bangladesh, Egypt, Jordan, Nigeria, Poland, Turkey and Vietnam.[9]
Affected areas	A level 7 nuclear accident would have widespread health and environmental effects. It could also have an impact on food and energy supply as well as on the economy of the region.
Affected regions	All regions near nuclear power plants and all regions downwind of the power plants would be affected. Depending on the distance from the nuclear accident and the meteorological conditions the impact could be disastrous.
Affected domain	It affects the nuclear and environmental domain.
Entry period	As long as there are nuclear power plants in the world this threat persists.
Application period	
Empirical values	An interdisciplinary team from MIT have estimated that given the expected growth of nuclear power from 2005–2055, at least four serious nuclear power accidents would be expected in that period.[10] A comparison of real accident statistics for severe accidents (defined as those resulting in 5 or more prompt fatalities) with the theoretically calculated accident statistics of nuclear power plants show that nuclear energy presents very much lower risks. For example between 1969 and 2000 there were 2259 and 3713 fatalities in the coal and oil energy chains respectively in OECD countries and 18 017 and 16 505 fatalities in non-OECD countries. Hydropower was responsible for 29 924 deaths in one incident in China. In contrast there has only been one severe accident in nuclear power plants over this period of time (Chernobyl) which resulted in 31 fatalities.[11] Assessment of the delayed (latent) fatalities associated with the exposure of radioactive material released by the Chernobyl accident indicates numbers up to 33 000 over the next 70 years. On this basis, natural background radiation would result in 1 500 times as many deaths (about 50 million) over the same timescale, so these additional fatalities, would be very difficult to observe.[11]
Source	http://en.wikipedia.org/wiki/Loss_of_coolant#cite_note-1. http://en.wikipedia.org/wiki/Criticality_accident. http://en.wikipedia.org/wiki/Decay_heat. http://en.wikipedia.org/wiki/Nuclear_and_radiation_accidents. Benjamin K. Sovacool. A Critical Evaluation of Nuclear Power and Renewable Electricity in Asia Journal of Contemporary Asia, Vol. 40, No. 3, August 2010, pp. 393–400. http://www.iaea.org/Publications/Factsheets/English/ines.pdf. "Analysis: A month on, Japan nuclear crisis still scarring" International Business Times (Australia). 9 April 2011. http://www.time.com/time/photogallery/0,29307,1887705,00.html. http://www.iaea.org/newscenter/statements/2013/amsp2013n05.html. Massachusetts Institute of Technology (2003). "The Future of Nuclear Power". p. 48. http://www.oecd-nea.org/ndd/reports/2010/nea6862-comparing-risks.pdf.

Title	**Nuclear tests**
Description	**Origin of threat:** manmade **Motives:** Testing nuclear weapons can yield information about how the weapons work. Additionally, nuclear testing has often been used as an indicator of scientific and military strength, and many tests have been overtly political in their intention.[1] **Methods:** Nuclear weapons tests have historically been broken into four categories:[1] • *Atmospheric testing* designates explosions that take place in the atmosphere. Generally these have occurred as devices detonated on towers, balloons, barges, islands, or dropped from airplanes. Nuclear explosions that are close enough to the ground can generate large amounts of nuclear fallout. • *Underground testing* refers to nuclear tests that are conducted under the surface of the earth, at varying depths. 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 as a consequence. Underground testing can result in seismic activity depending on the yield of the nuclear device and the composition of the medium it is detonated in, and generally result in the creation of subsidence craters.[2] • *Exoatmospheric testing* refers to nuclear tests conducted above the atmosphere. The test devices are lifted on rockets. These high altitude nuclear explosions can generate a

Nuclear electromagnetic pulse (NEMP), and charged particles resulting from the blast can cross hemispheres to create an auroral display.

- *Underwater testing* results from nuclear devices being detonated underwater, usually moored to a ship or a barge. 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 were widely dispersed in the atmosphere and deposited everywhere on the Earth's surface.[3]

It is difficult to assess the number of deaths that might be attributed to radiation exposure from nuclear testing. Some studies and evaluations, including an assessment by Arjun Makhijani on the health effects of nuclear weapon complexes, estimate that cancer fatalities due to the global radiation doses from the atmospheric nuclear testing programmes of the five nuclear-weapon States amount to hundreds of thousands.[4]

Background: Nuclear weapons tests are experiments carried out to determine the effectiveness, yield, and explosive capability of nuclear weapons. Throughout the 20th century, most nations that have developed nuclear weapons have tested them.[1]

There are many proposed anti-nuclear explosion treaties, such as the Partial Nuclear Test Ban Treaty, and the Comprehensive Nuclear Test Ban Treaty. Most of these treaties were passed because scientists in many different countries noticed spikes in radiation levels in civilian areas. Human nuclear testing also contributed to the formation of the treaties.[1]

The *Partial Nuclear Test Ban Treaty* makes it illegal to detonate any nuclear explosion anywhere except underground, in order to reduce atmospheric fallout. Most countries have signed and ratified the Partial Nuclear Test Ban which went into effect in October 1963. Of the nuclear states, France, China, and North Korea have never signed the Partial Nuclear Test Ban Treaty.[5]

The 1996 *Comprehensive Nuclear-Test-Ban Treaty* (CTBT) bans all nuclear explosions everywhere, including underground. For that purpose, the Preparatory Commission of the Comprehensive Nuclear-Test-Ban Treaty Organization is building an international monitoring system with 337 facilities located all over the globe. 85% of these facilities are already operational.[6]

As of May 2012, the CTBT has been signed by 183 States, of which 157 have also ratified. However, for the Treaty to enter into force it needs to be ratified by 44 specific nuclear technology-holder countries. The ratification of eight of these "Annex 2 states" is still missing: China, Egypt, Iran, Israel and the United States have signed but not ratified the Treaty; India, North Korea and Pakistan have not signed it.[7]

Future Importance:

Even after the Comprehensive Nuclear-Test-Ban Treaty was opened for signature in September 1996, about half a dozen nuclear tests have been conducted:[8]

- India conducted two tests in 1998
- Pakistan conducted two tests in 1998.
- The Democratic People's Republic of Korea announced that it had conducted a nuclear test in 2006, one in 2009 and again in 2013.

In January 2013, it was announced by North Korea that it plans to conduct further tests involving rockets that can carry satellites as well as nuclear warheads.[9]

Affected areas	The main impact is the exposure of the world's population to radiation.
Affected regions	Over 2,000 nuclear explosions have been conducted, in over a dozen different sites around the world: Russia/Soviet Union, France, United States, Great Britain, Israel, China, India, Pakistan and North Korea.[10]
Affected domain	Nuclear tests affect the health and environment domain.
Entry period	The first nuclear test was performed in 1945 by the US army.[1]
Application period	The most recent test was announced on 12 February 2013 - North Korean state media stated that it had conducted an underground nuclear test.[11]
Empirical values	
Source	http://en.wikipedia.org/wiki/Nuclear_weapons_testing http://www.globalsecurity.org/wmd/systems/nuke-testing.htm http://www.unscear.org/docs/reports/gareport.pdf http://www.armscontrol.org/act/2005_07-08/Makhijani http://www.state.gov/t/isn/4797.htm http://www.ctbto.org/fileadmin/user_upload/public_information/CTBT_Ending_Nuclear_

Explosions_web.pdf
http://www.ctbto.org/the-treaty/status-of-signature-and-ratification/
KIM, HYUNG-JIN (24 January 2013). "N. Korea Warns of Nuke Test, More Rocket Launches". U.S. News and World Report..
http://en.wikipedia.org/wiki/File:Rael_Nuclear_use_locations_world_map.png
http://en.wikipedia.org/wiki/2013_North_Korean_nuclear_test

Title	**Nuclear decommissioning**
Description	**Origin of threat:** manmade or accidents

Origin of threat: manmade or accidents

Motives: Either there is no motive at all (accidents, natural hazards or human errors) or there is the motive to steal nuclear material with a malicious intent.

Methods:

- Accidents and human errors
- Fires and floods
- Sabotage
- Theft of nuclear material (terroristic threat)

Impacts:

Each decommissioning is associated with particular technical challenges and risks to human health and the environment.[1]

The risks of large-scale *releases of radioactivity* during decommissioning are much lower than during a reactor's operations. However, the non-routine and hands-on nature of the work means risks related to worker exposure are higher during decommissioning than during operations.[1] Moreover, the risks associated with radioactive leaks due to human errors might be higher during decommissioning. Indeed, the perception of risk is lower after the spent fuel has been removed. In fact, the risk is not negligible due in part to the process being unregulated.[2]

Waste stored on-site poses potential risks if the storage equipment suffers corrosion or dissolution, or in case of fire. There are also risks related to fires or floods at decommissioning sites that release radioactive materials to the air, soil or groundwater (for instance, from areas where waste is processed or stored). If water penetrates the disposal site, it can dissolve radioactive isotopes and transport them to the water system.[1]

The *health risks facing workers* involved in decommissioning nuclear facilities are a critical concern as the nuclear weapons complex and nuclear power plants begin to be dismantled. In addition to risks from exposure to radioactive materials, there are risks from other common industrial materials like crystalline silica dust and asbestos.[3]

But where facilities are under decommissioning, and in particular when they are placed in "safe-store" mode or entombed, site surveillance has to be maintained to protect the contents from *theft and malicious use*. Concerns exist about the risks associated with the possible use of nuclear devices created from stolen nuclear material as well as sabotage of power stations.[4]

Since few NPPs have been fully decommissioned, the exact *costs* of accomplishing this phase are unknown.[5] Estimates vary from 9% to 200% of the construction costs.[6] A report by the Committee of Public Accounts (PAC) said the costs of decommissioning Sellafield nuclear power plant are £67.5 billion and still rising.[7]

Decommissioning in the aftermath of a major accident such as Three Mile Island (the United States), Chernobyl (Ukraine) or Fukushima (Japan) is quite different from planned decommissioning at the end of a facility's lifetime.[1]

Background:

Nuclear decommissioning is the dismantling and decontamination of a nuclear power plant site so that it will no longer require measures for radiation protection. The presence of radioactive material necessitates special precautions not required for the dismantling of other types of power plants.[8]

The International Atomic Energy Agency has defined three options for decommissioning, the definitions of which have been internationally adopted:[9]

- *Immediate Dismantling*: This option allows for the facility to be removed from regulatory control relatively soon after shutdown or termination of regulated activities. Usually, the final dismantling or decontamination activities begin within a few months or years, depending on the facility. Following removal from regulatory control, the site is then available for re-use.
- *Safe Enclosure*: This option postpones the final removal of controls for a longer

	period, usually in the order of 40 to 60 years. The facility is placed into a safe storage configuration until the eventual dismantling and decontamination activities occur.
	• *Entombment*: This option entails placing the facility into a condition that will allow the remaining on-site radioactive material to remain on-site without the requirement of ever removing it totally. This option usually involves reducing the size of the area where the radioactive material is located and then encasing the facility in a long-lived material such as concrete, that will last long enough to ensure the remaining radioactivity is no longer of concern.
	Future Importance:
	There are plans to close up to 80 civilian nuclear power reactors in the next ten years. While many of these reactors are likely to have their operating licenses extended, they will eventually be decommissioned.[1]
	Overall, decommissioning reactors will become a major operation over the next 50 years, with far-reaching implications including an increase in the production of radioactive waste, health and security issues, socio-economic impacts and inevitable technical challenges [10] (see empirical values).
Affected areas	
Affected regions	Regional distribution of nuclear power plants:[11]
	Africa 2 Asia - Middle East and South 24
	America – Latin 6 Europe – Central and Eastern 68
	America – Northern 121 Europe – Western 118
	Asia –Far East 97
Affected domain	It affects the health & environment domain as well as the nuclear domain itself.
Entry period Application period	Currently there are 436 nuclear power reactors in operation and 69 in construction. All of them will eventually be decommissioned.[11]
Empirical values	As of January 2012, 138 civilian nuclear power reactors had been shut down in 19 countries, including 28 in the United States, 27 in the United Kingdom, 27 in Germany, 12 in France, 9 in Japan and 5 in the Russian Federation. [12] Until 2012 decommissioning had only been completed for 17 of them.[1]
Source	http://www.unep.org/yearbook/2012/pdfs/UYB_2012_CH_3.pdf
	Iguchi Y & Kato M 2010. Risk-Informed Approach for the Regulation of Decommissioning of Nuclear Facilities. J. Eng. Gas Turbines Power, Vol 132, no 10, pp102910-102919.
	Dodic-Fikfak M, Clapp R, Kriebel D., The health risks of decommissioning nuclear facilities, New Solut. 1999;9(2):153-61.
	Bunn M and Bunn G 2008. Reducing the threat of nuclear theft and sabotage IAEA-SM-367/4/08, Interna-tional Atomic Energy Agency http://www.iaea.org/newscenter/features/nuclear_terrorism/bunn02.pdf.
	Ramana M V 2009. Nuclear Power: Economic, Safety, Health, and Environmental Issues of Near-Term Technologies Annual Review of Environment and Resources, vol. 34, pp 127-152.
	Lenzen M 2008. Life cycle energy and greenhouse gas emissions of nuclear energy: A review. Energy Conversion and Management, vol. 49, no. 8, pp 2178-2199.
	http://www.supplymanagement.com/news/2013/taxpayers-bear-risk-on-nuclear-decommissioning-contracts/
	http://en.wikipedia.org/wiki/Nuclear_decommissioning
	http://www.world-nuclear.org/info/Nuclear-Fuel-Cycle/Nuclear-Wastes/Decommissioning-Nuclear-Facilities/#.UaxUZnfc4Xg
	http://na.unep.net/geas/getuneppagewitharticleidscript.php?article_id=70
	http://www.iaea.org/pris/
	IAEA (2012). Power Reactor Information System Website. http://www.iaea.org/programmes/a2/

Title	**Nuclear material transportation**
Description	**Origin of threat:** manmade/ accidental
	Motives:
	The security threat is one of either unauthorized possession, theft of the material for illicit use later, or sabotage to cause incidents on the site, e.g. by dispersing the material to the environment.
	Methods:

	In fact, the vast majority of hazardous material transports - around 95% - are not fuel cycle related. Radioactive materials are used extensively in medicine, agriculture, research, manufacturing, non-destructive testing and in the exploration of minerals. A few incidents have occurred when radioactive material was disposed of improperly, shielding during transport was defective. Transport of nuclear weapons and materials is a particular concern, as it is the part of the nuclear material life-cycle most vulnerable to violent, forcible theft, since it is impossible to protect the material with thick walls when it is on the road. **Impacts:** Transport accidents can cause a release of radioactivity resulting in contamination or shielding to be damaged resulting in direct irradiation. In Cochabamba a defective gamma radiography set was transported in a passenger bus as cargo. The gamma source was outside the shielding, and it irradiated some bus passengers. In the United Kingdom, it was revealed in a court case that in March 2002 a radiotherapy source was transported from Leeds to Sellafield with defective shielding. The shielding had a gap on the underside. It is thought that no human has been seriously harmed by the escaping radiation. Inadvertent movement, without appropriate controls, can lead to the exposure of persons to radiation or to poisoning by chemical substances associated with the radioactive material. **Background:** A range of protection measures has been employed during transport, as deemed appropriate, ranging from the design of the package and the vehicles used as well as security forces, access control, employee screening, satellite tracking of shipments and coordination with local and national security authorities. The objectives of the requirements of physical protection of such materials during transport is assisted by minimizing both the total time the material remains in transport and the number and duration of transfers of the material, avoiding the use of regular movement schedules and limiting the advance knowledge of transport information including date of departure, route and destination to designated officials having a need to know that information. **Future Importance:** In the near future, because of a potential high-level waste repository being built, the number of shipments by road and rail is expected to increase.
Affected areas	Denials and delays of shipment of radioactive materials continue to occur, with the most apparent increase in denials of shipment resulting from national variations in regulations. Variations in regulations can create a level of complexity for different modes of transport that can increase the risk of undeclared dangerous goods, or miss-declared dangerous good creating problems for all parties involved in the supply chain.
Affected regions	Each day thousands of shipments of radioactive materials are transported around the world. These consignments which are carried by road, rail, air, sea and inland waterways can range from smoke detectors, cobalt sources for medical uses, to nuclear fuel cycle materials for electricity generation. (As of 2009, many countries were party to one or more of the 20 international or regional instruments facilitating the safe movement of goods, including radioactive materials. However, some conventions overlap and cover the same aspects of the transport journey.)
Affected domain	This threat is only relevant in the nuclear context.
Entry period	
Application period	
Empirical values	
Source	http://www-pub.iaea.org/MTCD/publications/PDF/pub1348_web.pdf http://www.wnti.co.uk/nuclear-transport-facts/security.aspx http://www.iaea.org/About/Policy/GC/GC55/GC55InfDocuments/English/gc55inf-3_en.pdf http://www.nrc.gov/waste/spent-fuel-transp.html

Title	**Theft of nuclear material/ International organized crime and illegal trafficking**
Description	**Origin of threat:** manmade **Motives:**

Where information on motives is available, it indicates that profit seeking is the principal motive behind theft, illegal trafficking and organized crime. Some cases, however, showed an indication of malicious intent:

- In most cases profit-motivated sellers hope to deceive unsophisticated buyers in the context of economic downturns affecting the Newly Independent States (NIS) and Eastern Europe.
- Terrorist groups are prepared to use the most violent and indiscriminate means to pursue their aims.

The threats involve criminals or terrorists acquiring and using for malicious purposes:

(a) nuclear explosive devices;

(b) nuclear material to build an improvised nuclear explosive device;

(c) radioactive material to construct a radiological dispersal device (RDD);

(d) the dispersal of radioactivity through sabotage of installations in which nuclear and other radioactive material can be found or of such material in transport.

There is a broad spectrum of threats that involve different types of radionuclides, of amounts of material, and of technical complexity.

Methods:

Advances in information technology and the availability of radioactive material have increased the likelihood that a terrorist or other criminal organization could obtain the necessary material, components and expertise to construct a nuclear explosive device or RDD. The radioactive sources for an RDD that could easily be accessible are those not under regulatory control. This may be because it has never been under regulatory control, or because it has been abandoned, lost, misplaced, stolen or transferred without proper authorization. Numerous incidents and accidents, including the accident in Goiânia, have occurred where equipment containing radioactive material has been discarded without due care and with no record or proper transfer of custody. However, radioactive sources that are not under regulatory control could be appropriated by traffickers and transferred to persons or organizations that might wish to use them malevolently.

Information on incidents involving illegal possession shows predominantly opportunistic and amateurish activities. As a result of unprofessional methods usually used to smuggle and offer the material for sale, such activities are more susceptible to detection. Well-organized trafficking networks using established channels for smuggling in other illegal goods will be more difficult to detect and interdict. There have been over 18 documented cases of theft or loss of plutonium or highly enriched uranium (HEU), the essential ingredients of nuclear weapons. Russian officials have confirmed that terrorist teams have carried out reconnaissance at Russian nuclear weapon storage facilities.

Impacts:

A major threat recognized at the conference on nuclear security in London, in 2005, is that unauthorized persons or groups may acquire radioactive material for use in RDDs, or 'dirty bombs'. These devices combine radioactive material with conventional explosives and, when detonated, could disperse the radioactive material over a wide area, contaminating persons, property and the environment.

Illicit trafficking and theft of nuclear material can lead to nuclear proliferation and the possible construction of improvised nuclear devices or radiological dispersal and exposure devices.

Background:

Of the incidents reported by States, about 54% show evidence of criminal activity, such as theft, illegal possession and attempts to sell or smuggle nuclear or radioactive material across national borders. The number of such incidents reported declined sharply between 1994 and 1996, but since then it has been gradually increasing. Thefts have involved primarily sealed industrial radioactive sources, e.g. sources used in gauges or radiography devices. Reports of theft have been gradually increasing since 1998. The intentions and motives behind the thefts are very difficult to determine.

Of the 150 incidents that occurred in 2006, 14 involved unauthorized possession and related criminal activities and can be described as illicit trafficking, containing such factors as illegal possession, movement, or attempts to illegally trade in the materials. The majority of these incidents involved sealed radioactive sources and the materials included natural uranium, depleted uranium, and thorium. Another 85 incidents in 2006 involved thefts, losses or misrouting of nuclear or other radioactive materials. Thefts of such materials are of particular concern since they can be upstream evidence of illicit trafficking and are indicators of vulnerabilities in control and security systems. In about 73 per cent of cases, the lost or stolen materials have not been reportedly recovered. Eight

	of these incidents involved high-risk "dangerous" radioactive sources that are classified as Category 2 and 3. Another 51 reported incidents involved various types of material recovery showing no direct evidence of criminal behavior, such as detection of materials disposed of in an unauthorized way. The problem of criminal or unauthorized acts involving nuclear and other radioactive material is compounded by the prevalence of incidents dealing with false representations of nuclear or other radioactive material. Many such cases consist of hoaxes or scams that either falsely claims the presence of radionuclides that do not exist or misrepresent the nature or quantity of trafficked material. **Future Importance:** Information reported to the ITDB shows a persistent problem with the illicit trafficking in nuclear and other radioactive materials, thefts, losses, and other unauthorized activities. (ITDB report 2007)
Affected areas	In addition to the long recognized threat of the horizontal proliferation of nuclear weapons, the possibility that non-State actors might engage in nuclear or radiological terrorism has become a matter of rising concern for States and international organizations. The immense length of national borders, the huge scale of legitimate traffic, the myriad potential pathways across these borders, and the small size and weak radiation signal of the materials needed to make a nuclear bomb make nuclear smuggling extraordinarily difficult to stop.
Affected regions	The IAEA Illicit Nuclear Trafficking Database notes 1,266 incidents reported by 99 countries over the last 12 years, including 18 incidents involving HEU or plutonium trafficking. It appears that the highest risks of nuclear theft today are in: • Pakistan, where a small and heavily guarded nuclear stockpile faces immense threats, both from insiders who may be corrupt or sympathetic to terrorists and from large-scale attacks by outsiders; • Russia, which has the world's largest nuclear stockpiles in the world's largest number of buildings and bunkers; security measures that have improved dramatically but still include important vulnerabilities (and need to be sustained for the long haul); and substantial threats, particularly from insiders, given the endemic corruption in Russia; and • HEU-fueled research reactors, which usually (though not always) use only modest stocks of HEU, in forms that would require some chemical processing before they could be used in a bomb, but which often have only the most minimal security measures in place - in some cases little more than a night watchman and a chain-link fence. Nuclear security issues exist not only in developing and transition countries but in wealthy countries as well, some of which have no armed guards at nuclear facilities, or only protect these facilities against very modest threats.
Affected domain	This threat is only relevant in the nuclear context.
Entry period	
Application period	
Empirical values	In January 2007, Georgia reported to the ITDB an incident that occurred in February 2006 and involved the seizure of 79.5 grammes of 89 per cent-enriched uranium. As of 31 December2006, the ITDB contained 1,080 confirmed incidents reported by participating States since 1993, of which 275 involved unauthorized possession and related criminal activity, 332 involved thefts or loss and 398 other unauthorized activities. (http://www.un.org/apps/news/story.asp?NewsID=23774#.Uaw6rndhuW8) As of 31 December 2006, States had reported a total of 1080 incidents of illicit trafficking and other unauthorized activities involving nuclear and other radioactive material to the ITDB. Of these, about 25% involved nuclear material and about 70% other radioactive material, mainly sealed radioactive sources. The remainder involved radioactively contaminated and other material. Figure 21 shows the distribution of incidents reported to the ITDB between 1993 and 2006 by type of material. In addition, there are numerous incidents reported in open sources which have not yet been confirmed or otherwise commented on to the ITDB by the States concerned. (http://www-pub.iaea.org/MTCD/publications/PDF/pub1309_web.pdf) More than 250 incidents involving unauthorized possession and related criminal activities, theft or loss of nuclear or other radioactive materials, and other activities such as

	unauthorized disposal of radioactive materials were reported to the UN International Atomic Energy Agency (IAEA) Illicit Trafficking Database (ITDB), of which 150 occurred in 2006 and the rest mainly in 2005.
Source	http://www.wnti.co.uk/nuclear-transport-facts/security.aspx http://www.un.org/apps/news/story.asp?NewsID=23774#.Uaw6rndhuW8 http://www-pub.iaea.org/MTCD/publications/PDF/pub1309_web.pdf http://en.wikipedia.org/wiki/Nuclear_and_radiation_accidents http://www.nti.org/media/pdfs/Securing_The_Bomb_2010.pdf?_=1317159794

Title	**Uranium mining**
Description	**Origin of threat:** manmade **Motives:** Uranium is needed among other things for nuclear power plants. **Methods:** • Insufficient safety measures • Lack of training of the workers **Impacts:** Uranium ore itself is relatively harmless, but through the mechanical extraction of uranium ore, miners are exposed not only to fine particles of uranium but also to radon. The inhalation of uranium particles and radon can cause cancer, particularly in the lungs.[1] One of the dangers that the tailings pose is the contamination of groundwater through the porous separating layers, erosion and seeping rainwater. Erosion through wind carries radioactive particles and radon many kilometres away from the heaps. [1] The immense amount of water that is required by uranium mining represents another problem; e.g. it was stated that the uranium mines of Niger used 270 billion litres of water over 40 years of operation. After its use the contaminated water was dumped back into rivers and lakes.[2] In producer countries it is the indigenous population that suffers most from the effects of uranium mining. Apart from direct effects, there are also severe cultural and religious consequences, e.g. the mining on indigenous people's sacred sites. Cultural procedures, such as the way they feed themselves and rites are also disturbed. The means of subsistence are destroyed by the contamination of land and water. These developments affect, for instance, the Tuareg in Niger, the Uraon in Laos, the Navajos and Lakotas in the USA and the aborigines in Australia.[3] On the other hand, in western countries the health risks due to uranium mining seem to be negligible. The Nuclear Energy Institute (NEI) claims that safety standards and improved operating practices have lowered radon exposure among works dramatically since the early years of mining. They say that the concentration of radon gas in mines is monitored by the Mine Safety and Health Administration (MSHA) and that all underground mines have extensive ventilation systems, incorporating multiple vertical shafts and fans, to bring fresh air into the mines.[4] Jay Lehr from the Heartland Institute concluded that based on the proven effective approach in Canada, Western US and Australia an extensive regulatory regime exists to protect miners, people living near the mine and the general public from any emissions, radioactive or otherwise, that might come from the mine or the processing of its output.[5] The Canada Nuclear Safety Commission stated that uranium mine workers have the lowest injury rates in the Canadian mining industry and modern workers are no less healthy that the average Canadian citizen.[6] In the Western Countries these health risks still remain an issue for those who have been employed in the past. Many uranium miners in the Four Corners region[7] contracted lung cancer and other pathologies as a result of high levels of exposure to radon in the mid-1950s.[8] Despite efforts made in cleaning up uranium sites, significant problems stemming from the legacy of uranium development still exist today on the Navajo Nation and in the states of Utah, Colorado, New Mexico, and Arizona. Hundreds of abandoned mines have not been cleaned up and present environmental and health risks in many communities.[9] **Background:** Uranium mining is the process of extraction of uranium ore from the ground. The worldwide production of uranium in 2009 amounted to 50,572 tonnes.[10] A prominent use of uranium from mining is as fuel for nuclear power plants.[11] As of 2008, known uranium ore resources that can be mined at about current costs are estimated to be sufficient to produce fuel for about a century, based on current consumption

	rates.[12] **Future Importance:** Globally, nuclear power looks set to continue to grow steadily, although more slowly than it was expected before the Fukushima Daiichi accident. There are 437 operating nuclear power reactors in the world today. The latest IAEA projections suggest that number could increase by 80 or 90 in the next 20 years. It could even double.[13] This increased need for nuclear power implies an increased need for uranium mining.
Affected areas	
Affected regions	According to the Nuclear Energy Agency and the International Atomic Agency (IAEA) only seven countries have a capacity to export uranium worth speaking of.[14] The biggest producer of natural uranium worldwide is Kazakhstan, accounting for 27.4% of global production. Then Canada follows with 20.1% and Australia with 15.7% of the market. Namibia and South Africa are counted together and are on the fourth place, followed by Russia with about 7% of the global market. Niger, Uzbekistan and the USA are the other large producers.[15]
Affected domain	It affects the nuclear and environmental domain.
Entry period Application period	As long as the population needs uranium for nuclear power plants, there will be health risks and threats to the cultural heritage at some sites.
Empirical values	The Saskatchewan Uranium Miners Cohort Study calculated that about 24,000 workers will have spent time working at an uranium mine by the year 2030. During this period, 141 miners could be expected to develop lung cancer, primarily from tobacco smoking. Only one (1) additional miner could expect to get lung cancer from exposure to RDP in the workplace. The study concluded that it would not be feasible to investigate the risk of excess lung cancer in modern miners because exposures are so low. It would also be practically impossible to accurately correct for the effects of smoking and residential radon, factors that could greatly impact the study results.[16] The UNSCEAR report also concludes that the power to detect any excess risks in miners nowadays is likely to be small, as the exposures are much smaller than in the early years of mining.[17] There are no empirical values available from Niger. But it was stated that[18] • Waste dumps and related processing facilities are posing a severe environmental and health hazard to the local population of approximately 80,000. • Contaminated construction materials have been sold on local markets and were found in dwellings and in the towns. • There is evidence of radioactive contamination of local water supplies, and contaminated dust is accumulating throughout the two villages. • Workers' protection and compensation for occupational illnesses is non-existent.
Source	Fact Sheet Uranium Mining 4, Uranium Mining, Health and Indigenous Peoples, Preconference of the IPPNW-World congress 26 August 2010, University of Basel. Greenpeace International, Report „Left in the Dust – Areva's radioactive legacy in the desert towns of Niger", Mai 2010. Fact Sheet Uranium Mining 1, Uranium Mining, Health and Indigenous Peoples, Preconference of the IPPNW-World congress 26 August 2010, University of Basel. Nuclear Energy Institute, Fact Sheet, „Radon Safety measures in uranium mining", August 2012. Jay Lehr, Uranium Mining in Virginia: Environmental Safety Considerations, The Heartland Institute, Jan. 2013. http://www.amebc.ca/policy/land-access-and-use/uranium-exploration.aspx. south-western corner of Colorado, north-western corner of New Mexico, north-eastern corner of Arizona and south-eastern corner of Utah Roscoe, R. J.; Deddens, J. A.; Salvan, A.; Schnorr, T. M. (1995). "Mortality among Navajo uranium min-ers". American Journal of Public Health 85 (4): 535. doi:10.2105/AJPH.85.4.535. PMC 1615135. PMID 7702118. Pasternak, Judy (2006-11-19). "A peril that dwelt among the Navajos". Los Angeles Times. "World Uranium Mining". World Nuclear Association. http://en.wikipedia.org/wiki/Uranium_mining#cite_note-2 "Uranium resources sufficient to meet projected nuclear energy requirements long into the future". Nuclear Energy Agency (NEA). 3 June 2008. http://www.iaea.org/newscenter/statements/2013/amsp2013n05.html.

	NEA/IAEA, Uranium 2007 (2008).
	Fact Sheet Uranium Mining 2, Uranium Mining, Health and Indigenous Peoples, Preconference of the IPPNW-World congress 26 August 2010, University of Basel.
	http://nuclearsafety.gc.ca/eng/readingroom/healthstudies/feasibility-study-saskatchewan-uranium-miners-cohort-study.cfm
	"UNSCEAR 2006 Report Vol. I". United Nations Scientific Committee on the Effects of Atomic Radiation UNSCEAR 2006 Report to the General Assembly, with scientific annexes.
	http://www.tagesspiegel.de/downloads/8246666/1/Areva%20Uranminen

Title	**Nuclear espionage**
Description	**Origin of threat:** manmade, intentional attack
	Motives: Nuclear espionage is the purposeful giving of state secrets regarding nuclear weapons to other states without authorization (espionage). During the history of nuclear weapons there have been many cases of known nuclear espionage, and also many cases of suspected or alleged espionage. Because nuclear weapons are generally considered the most important state secrets, all nations with nuclear weapons have strict restrictions against the giving of information relating to nuclear weapon design, stockpiles, delivery systems, and deployment. States are also limited in their making public of weapons information by non-proliferation agreements. However either nations or terrorists have a strong interest to increase their power with nuclear technology in general and weapons technology more specific.
	Methods: In addition to classical intelligence methods, nuclear espionage is often combined with scientific knowledge exchange, organized crime, corruption and terrorism. In transforming nations like Russia are a remarkable number of nuclear experts unemployed and there is a potential illegal knowledge transfer. In addition to these social drivers, methods from cyber espionage are useful for nuclear espionage. Stuxnet has proven, that it is possible to enter the scada systems from nuclear facilities. It is very likely, that some next generation Trojans will be developed for data retrieval in nuclear research.
	Impact: Successful nuclear espionage will lead to a wide distribution of knowledge about nuclear weapons, at least for the person, who are looking fur such information.
	Background: In a 1999 report of the United States House of Representatives Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, chaired by Rep. Christopher Cox (known as the Cox Report), it was revealed that U.S. security agencies believed that there is an on-going nuclear espionage by the People's Republic of China (PRC) at U.S. nuclear weapons design laboratories, especially Los Alamos National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, and Sandia National Laboratories. According to the report, the PRC had "stolen classified information on all of the United States' most advanced thermonuclear warheads" since the 1970s, including the design of advanced miniaturized thermonuclear warheads (which can be used on MIRV weapons), the neutron bomb, and "weapons codes" which allow for computer simulations of nuclear testing (and allow the PRC to advance their weapon development without testing themselves).
	In January 2004, Dr. Abdul Qadeer Khan confessed to selling restricted technology to Libya, Iran, and North Korea. According to his testimony and reports from intelligence agencies, he sold designs for gas centrifuges (used for uranium enrichment), and sold centrifuges themselves to these three countries. Khan had previously been indicated as having taken gas centrifuge designs from a uranium enrichment company in the Netherlands (URENCO) which he used to jump-start Pakistan's own nuclear weapons program. On February 5, 2004, the president of Pakistan, General Pervez Musharraf, announced that he had pardoned Khan. Pakistan's government claims they had no part in the espionage, but refuses to turn Khan over for questioning by the International Atomic Energy Agency..
	Relevance in the future: It can be expected, that all types of information will diffuse to other user in a much higher speed than today. Even if the information is very well protected, for the time being, this is not a guaranty to keep this safe situation in the future. Professional spies, either with or without national support, will work on colleting all kind of valuable information, in the future and deal with this on online black markets for information. Nuclear information is very well protected for the time being, but there is no guaranty, that this will be the same in the future. In the opposite, there are some weak

	signals, that even the best protected national secrets will enter a room for illegal information exchange at some point of time in the future. E.g., it was possible for the Khan network, to deals with such type of information.
Affected areas	The threat has some impact on the trustfulness of nuclear service provider.. For the the citizens, it is a lost in freedom. and a very effective way, to build up effective counter measures.
Affected regions	This attack is suitable for asymmetric warfare.
Affected domain	Nuclear service provider and nuclear researchers are primarily affected, by this threat.
Entry period	10-50 years.
Application period	Since now and open end.
Empirical values	Only national secrets maturity of nuclear research.
Sources	**weak signals**: stuxnet, ghost net, zero day exploits, cyber attack unites Wikipedia, http://www.house.gov/coxreport/, Powell, Bill, and Tim McGirk. "The Man Who Sold the Bomb; How Pakistan's A.Q. Khan outwitted Western intelligence to build a global nuclear-smuggling ring that made the world a more dangerous place", Time Magazine (14 February 2005), Organized Crime: From Trafficking to Terrorism, Band 1, herausgegeben von Frank G. Shanty,Patit Paban Mishra

Title	**Nuclear espionage**
Description	**Origin of threat:** manmade, intentional attack **Motives:** Nuclear espionage is the purposeful giving of state secrets regarding nuclear weapons to other states without authorization (espionage). During the history of nuclear weapons there have been many cases of known nuclear espionage, and also many cases of suspected or alleged espionage. Because nuclear weapons are generally considered the most important state secrets, all nations with nuclear weapons have strict restrictions against the giving of information relating to nuclear weapon design, stockpiles, delivery systems, and deployment. States are also limited in their making public of weapons information by non-proliferation agreements. However either nations, or terrorists have a strong interest to increase their power with nuclear technology in general and weapons technology more specific. **Methods:** In addition to classical intelligence methods, nuclear espionage is often combined with scientific knowledge exchange, organized crime, corruption and terrorism. In transforming nations like Russia are a remarkable number of nuclear experts unemployed and there is a potential illegal knowledge transfer. In addition to these social drivers, methods from cyber espionage are useful for nuclear espionage. Stuxnet has proven that it is possible to enter the scada systems from nuclear facilities. It is very likely, that some next generation Trojans will be developed for data retrieval in nuclear research. **Impact:** Successful nuclear espionage will lead to a wide distribution of knowledge about nuclear weapons, at least for the person, who are looking for such information. **Background:** In a 1999 report of the United States House of Representatives Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, chaired by Rep. Christopher Cox (known as the Cox Report), it was revealed that U.S. security agencies believed that there is an on-going nuclear espionage by the People's Republic of China (PRC) at U.S. nuclear weapons design laboratories, especially Los Alamos National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, and Sandia National Laboratories. According to the report, the PRC had "stolen classified information on all of the United States' most advanced thermonuclear warheads" since the 1970s, including the design of advanced miniaturized thermonuclear warheads (which can be used on MIRV weapons), the neutron bomb, and "weapons codes" which allow for computer simulations of nuclear testing (and allow the PRC to advance their weapon development without testing themselves). In January 2004, Dr. Abdul Qadeer Khan confessed to selling restricted technology to Libya, Iran, and North Korea. According to his testimony and reports from intelligence agencies, he sold designs for gas centrifuges (used for uranium enrichment), and sold centrifuges themselves to these three countries. Khan had previously been indicated as having taken gas centrifuge designs from a uranium enrichment company in the Netherlands (URENCO) which he used to jump-start Pakistan's own nuclear weapons program. On February 5, 2004, the president of Pakistan, General Pervez Musharraf, announced that he had pardoned Khan. Pakistan's government claims they had no part in the espionage, but refuses to turn Khan over for questioning by the International Atomic

	Energy Agency..
	Relevance in the future: It can be expected, that all types of information will diffuse to other user in a much higher speed than today. Even if the information is very well protected, for the time being, this is not a guaranty to keep this safe situation in the future. Professional spies, either with or without national support, will work on colleting all kind of valuable information, in the future and deal with this on online black markets for information. Nuclear information is very well protected for the time being, but there is no guaranty, that this will be the same in the future. In the opposite, there are some weak signals, that even the best protected national secrets will enter a room for illegal information exchange at some point of time in the future. E.g., it was possible for the Khan network, to deals with such type of information.
Affected areas	The threat has some impact on the trustfulness of nuclear service provider. For the citizens, it is a lost in freedom and a very effective way, to build up effective counter measures.
Affected regions	This attack is suitable for asymmetric warfare.
Affected domain	Nuclear service provider and nuclear researchers are primarily affected, by this threat.
Entry period	10-50 years.
Application period	Since now and open end.
Empirical values	Only national secrets.naturity of nuclear research.
Sources	**weak signals**: stuxnet, ghost net, zero day exploits, cyber attack unites Wikipedia, http://www.house.gov/coxreport/, Powell, Bill, and Tim McGirk. "The Man Who Sold the Bomb; How Pakistan's A.Q. Khan outwitted Western intelligence to build a global nuclear-smuggling ring that made the world a more dangerous place", Time Magazine (14 February 2005), Organized Crime: From Trafficking to Terrorism, Band 1, herausgegeben von Frank G. Shanty,Patit Paban Mishra

Title	**Terroristic CBRN attack**
Description	**Origin of threat:** manmade, intentional attack **Motives:** An important motivation for terrorists is to generate pschical as much fear and physical damage, as possible, with as low effoert as possible to increase their media atention and their political influence. Al-Qa'ida and associated extremist groups often uses low technology methods for their attacks. Nevertheless, according to CIA, they are on the way to develop capabilities for chemical, biological, radiological, or nuclear (CBRN) attacks. Al-Qa'ida's end goal is the use of CBRN to cause mass casualties; however, most attacks by the group—and especially by associated extremists—probably will be small scale, incorporating relatively crude delivery means and easily produced or obtained chemicals, toxins, or radiological substances. The success of any al-Qa'ida attack and the number of ensuing casualties would depend on many factors, including the technical expertise of those involved, but most scenarios could cause panic and disruption. **Methods:** *Chemical agents* Terrorists have considered a wide range of toxic chemicals for attacks. Typical plots focus on poisoning foods or spreading the agent on surfaces to poison via skin contact, but some also include broader dissemination techniques. Typically, Cyanides, Mustard Agent and Nerve Agents, like Sarin, tabun, and VX are considered for a cemical attack. However, their synthesis requires significant chemical expertise. In the oposite to this, industrial chemicals are esear to aqieew. Chlorine and phosgene are industrial chemicals that are transported in multiton shipments by road and rail. Rupturing the container can easily disseminate these gases. The effects of chlorine and phosgene are similar to those of mustard agent. Organophosphate pesticides such as parathion are in the same chemical class as nerve agents. Although these pesticides are much less toxic, their effects and medical treatments are the same as for military-grade nerve agents. *Biological agents* Typical biological agents for a terroristic attack are Anthrax, Botulinum toxin and Ricin. They are relative easy in prodiction and very effective in poisoning. *Radiological Dispersal Devices (RDD) Improvised Nuclear Device (IND)* An RDD is a conventional bomb not a yield-producing nuclear device. RDDs are designed to disperse radioactive material to cause destruction, contamination, and injury from the radiation produced by the material. An RDD can be almost any size, defined only by the amount of radioactive material and explosives. A passive RDD is a system in which unshielded radioactive material is dispersed or placed manually at the target. An

explosive RDD—often called a "dirty bomb"—is any system that uses the explosive force of detonation to disperse radioactive material. An atmospheric RDD is any system in which radioactive material is converted into a form that is easily transported by air currents. A variety of radioactive materials is commonly available and could be used in an RDD, including Cesium-137, Strontium-90, and Cobalt-60. Hospitals, universities, factories, construction companies, and laboratories are possible sources for these radioactive materials.

An IND is intended to cause a yield-producing nuclear explosion. An IND could consist of diverted nuclear weapon components, a modified nuclear weapon, or indigenous-designed device. INDs can be categorized into two types: implosion and gun assembled. Unlike RDDs that can be made with almost any radioactive material, INDs require fissile material—highly enriched uranium or plutonium—to produce nuclear yield and thus are much more difficult in aquisition and production.

Impact: There are a number of different impacts possible in CBRN attacks. Chemical and biological agents usually have a short term impact on poisoning the contaminated location. Nuclear agents can either have a short term poisoning effect or a long term radioactive contamination effect. All CBRN attacks can result in health, environmental, or economic effects as well as political and social effects. They will cause fear, injury, and possibly lead to levels of contamination requiring costly and time-consuming cleanup efforts.

Background: Several groups of mujahidin associated with al-Qa'ida have attempted to carry out "poison plot" attacks in Europe with easily produced chemicals and toxins best suited to assassination and small-scale scenarios. These agents could cause hundreds of casualties and widespread panic if used in multiple simultaneous attacks.

Al-Qa'ida is interested in radiological dispersal devices (RDDs) or "dirty bombs." Construction of an RDD is well within its capabilities as radiological materials are relatively easy to acquire from industrial or medical sources. Usama Bin Ladin's operatives may try to launch conventional attacks against the nuclear industrial infrastructure of the United States in a bid to cause contamination, disruption, and terror.

A document recovered from an al-Qa'ida facility in Afghanistan contained a sketch of a crude nuclear device.

Spray devices disseminating biological warfare (BW) agents have the highest potential impact. Both 11 September attack leader Mohammad Atta and Zacharias Moussaoui expressed interest in crop dusters, raising our concern that al-Qa'ida has considered using aircraft to disseminate BW agents.

Analysis of an al-Qa'ida document recovered in Afghanistan in summer 2002 indicates the group has crude procedures for making mustard agent, sarin, and VX..

Relevance in the future: In the future it is expected, that terrorists extend their high technology and scientific capabilities and thus will improve their knowledge about production and use of CBRN agents.

Affected areas	Primarily affected are citizens in particular at mass events or places with high population density like mega cities.
Affected regions	All countries
Affected domain	Nuclear and environment
Entry period	There is an increasing probability, that CBRN attacks will be considered for asymmetric warfare.
Application period	Since now and open end.
Empirical values	Increasing communication and knowledge about CBRN in non-military research networks.
weak signals	Knowledge exchange networks between scientists and terrorists
Sources	https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm, Wikipedia

Title	**Nuclear waste storage**
Description	**Origin of threat:** manmade **Motives:** The security threat is one of either unauthorized possession, theft of the material for illicit use later, or sabotage to cause incidents on the site, e.g. by dispersing the material to the environment. **Methods:** Three types of risk should be taken into consideration:

- Risk of unauthorized removal with the intent to construct a nuclear explosive device;
- Risk of unauthorized removal which could lead to subsequent dispersal;
- Risk of sabotage (nuclear material and nuclear facilities).

While nuclear material has traditionally attracted security precautions to prevent it falling into unauthorized possession, it is now recognized that non-fissile material must also be protected because of the possible threat of deliberate spreading of contamination by terrorists. The material is obviously much more vulnerable to attack if placed on the surface. In geological disposal facilities, it is beyond the reach of all but the most determined and sophisticated of individuals or groups.

Attention should be paid to insiders. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures.

Examples:

Peace activists have broken into a Belgian base where U.S. nuclear weapons are reportedly stored and two teams of armed men attacked a site in South Africa where hundreds of kilograms of highly enriched uranium (HEU) are stored.

Impacts:

Unauthorized removal and sabotage could cause harm to human health and the environment, as well as economic loss.

Examples:

In the Soviet Union, waste stored in Lake Karachay was blown over the area during a dust storm after the lake had partly dried out. At Maxey Flat, a low-level radioactive waste facility located in Kentucky, containment trenches covered with dirt, instead of steel or cement, collapsed under heavy rainfall into the trenches and filled with water. The water that invaded the trenches became radioactive and had to be disposed of at the Maxey Flat facility itself. In other cases of radioactive waste accidents, lakes or ponds with radioactive waste accidentally overflowed into the rivers during exceptional storms. In Italy, several radioactive waste deposits let material flow into river water, thus contaminating water for domestic use. In France, in the summer of 2008 numerous incidents happened; in one, at the Areva plant in Tricastin, it was reported that during a draining operation, liquid containing untreated uranium overflowed out of a faulty tank and about 75 kg of the radioactive material seeped into the ground and, from there, into two rivers nearby; in another case, over 100 staff were contaminated with low doses of radiation.

Background:

As the result of delays in decisions on spent fuel disposal, the volume of spent fuel discharged from reactors needing to be stored is growing and, in an increasing number of cases, exceeding spent fuel pool capacities.

Long term surface storage is not the best option from the security point of view because spent nuclear fuel and high level wastes in surface storage are more vulnerable to theft and sabotage. Security considerations, which carry increasing weight, lead strongly and unequivocally to disposal being desirable at as early a date as is reasonable. Placing the waste material underground, even without finally closing the facility, greatly increases the difficulty of access to the material by unauthorized persons.

Safety of surface storage facilities will degenerate in the long term if active controls are not maintained.

Future Importance:

One of the greatest on-going challenges in the management of spent fuel and radioactive waste is the development and implementation of disposal strategies. In particular, geological disposal of radioactive waste and spent fuel remained a topic of concern.

However, progress has been made, in particular on technological and socio-political aspects. The lessons learned showed that progress in implementing disposal strategies required open and transparent dialogue among all interested parties in addition to well-founded scientific investigations and use of appropriate technologies.

Disposal of spent fuel and high level waste was a particular challenge and its implementation has been delayed in many countries. This indicated that there was a need for increased storage capacities and that the fuel will be stored for longer periods than initially intended. However, progress was made towards disposal notably in Sweden, Finland and France, where license applications are expected in 2011, 2012 and 2014, respectively.

The importance of having effective civil liability mechanisms in place to insure against harm to human health and the environment, as well as economic loss caused by nuclear

	damage, remains a subject of increased attention among States.
	Many countries have not yet defined a proper strategy to manage their current and future disused radioactive sources. This issue was and will continue to be of particular importance for countries that have a low volume of radioactive waste and no nuclear power programme.
	Long term safety also requires that future societies will be in a position to exercise active control over these materials and maintain effective transfer of responsibility, knowledge and information from generation to generation. Long term storage is only sustainable if future societies can maintain these responsibilities.
Affected areas	Irresponsibility on the part of the radioactive material's owners, usually a hospital, university or military, and the absence of regulation concerning radioactive waste, or a lack of enforcement of such regulations, have been significant factors in radiation exposures. For an example of an accident involving radioactive scrap originating from a hospital, see the Goiânia accident.
Affected regions	Of the 441 reactors currently operating around the world, many were built in the 1970s and 1980s, with an average lifespan of around 35 years. Their decommissioning peak will occur from 2020 to 2030 which will present a major managerial, technological, safety and environmental challenge to those States engaged in nuclear decommissioning. The need for national and international mechanisms for early planning, adequate funding and long term strategies applies not only to decommissioning, but also to radioactive waste management and spent fuel management, including disposal arrangements and clean-up, as well as the preservation of operational knowledge and experience to ensure the safety of these activities.
	Scavenging of abandoned radioactive material has been the cause of several other cases of radiation exposure, mostly in developing nations, which may have less regulation of dangerous substances (and sometimes less general education about radioactivity and its hazards) and a market for scavenged goods and scrap metal.
Affected domain	This threat is only relevant in the nuclear context.
Entry period	
Application period	
Empirical values	
weak signals	
Sources	http://www-pub.iaea.org/MTCD/publications/PDF/pub1348_web.pdf
	http://www.iaea.org/About/Policy/GC/GC55/GC55InfDocuments/English/gc55inf-3_en.pdf
	http://www-pub.iaea.org/MTCD/publications/PDF/LTS-RW_web.pdf
	http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf
	http://en.wikipedia.org/wiki/Radioactive_waste
	http://www.nti.org/media/pdfs/Securing_The_Bomb_2010.pdf?_=1317159794

Title	**Nuclear warfare**
Description	**Origin of threat:** manmade
	Motives: Nuclear warfare is used to inflict damage on an opponent. Compared to conventional warfare, nuclear warfare can be vastly more destructive in range and extent of damage, and in a much shorter time frame.[1]
	Methods:
	• Intentional conduction of atomic bombings
	• Accidental nuclear war (e.g. malfunctioning early warning devices, deliberate malfeasance by rogue military commanders, consequences of an accidental straying of warplanes into enemy airspace, reactions to unannounced missile tests during tense diplomatic periods, reactions to military exercises, mistranslated or miscommunicated messages)[1]
	Impacts:
	• Even a single nuclear explosion over a city can kill hundreds of thousands of people immediately. The casualties of a nuclear war in which even a small fraction of today's arsenals are used would reach into the tens of millions.[2]
	• Nuclear weapons eradicate the social infrastructure required for recovery from

<table>
<tr><td></td><td>conflict. Roads and transportation systems, hospitals and pharmacies, fire fighting equipment, and communications would all lie in rubble throughout a zone of complete destruction extending for miles.[2]

- Even a limited, regional nuclear war between India and Pakistan would cause significant climate disruptions worldwide. The resulting soot cloud would block 7-10% of warming sunlight, leading to significant cooling and reductions in precipitation lasting for more than a decade. Within 10 days following the explosions, there would be a drop in average surface temperature of 1.25°C.[3]
- A nuclear war using only a small fraction of current global arsenals would quickly cause prolonged and catastrophic stratospheric ozone depletion.[3]
- A massive nuclear exchange between the US and Russia would result in nuclear winter – a global ecological destruction. Among the effects would be a 45% global average reduction in precipitation and a global average surface cooling of -7°C and -8°C, which would persist for years.[3]
- What makes nuclear weapons uniquely abhorrent is the ionizing radiation they release as a result of the uncontrolled chain reaction of fissile materials. Exposure to ionizing radiation causes both acute (immediate) and long term health effects.[2]

Background:
There are eight states that have successfully detonated nuclear weapons. Five are considered to be "nuclear-weapon states" under the terms of the Nuclear Non-Proliferation Treaty (NPT). These are: the United States, Russia, the United Kingdom, France, and China. Three states were not parties to the Treaty, but have conducted nuclear tests, namely India, Pakistan, and North Korea. North Korea had been a party to the NPT but withdrew in 2003.[4] Israel is also widely believed to have nuclear weapons, though it has refused to confirm or deny this, and is not known definitively to have conducted a nuclear test.[5] South Africa has the unique status of a nation that developed nuclear weapons but has since disassembled its arsenal before joining the NPT.[1]

Future Importance:
A key development in nuclear warfare throughout the 2000s and early 2010s is the proliferation of nuclear weapons to the developing world, with *India and Pakistan* both publicly testing several nuclear devices.[1]
In the Persian Gulf, *Iran* appears to many observers to be in the process of developing a nuclear weapon, which has greatly heightened fears of a nuclear conflict and arms races in the Middle East—either with Israel or with one or more Arab states.[1]
Iran says its nuclear program is for peaceful civilian purposes, but American intelligence agencies and the International Atomic Energy Agency have picked up evidence in recent years that some Iranian research activities that may be weapons-related have continued since 2003, officials said.[6]
Israel is thought to possess somewhere between one hundred and four hundred nuclear warheads. Israel has been involved in wars with its neighbours in the Middle East on numerous prior occasions, and its small geographic size and population could mean that, in the event of future wars, the Israeli military might have very little time to react to an invasion or other major threat. Such a situation could escalate to nuclear warfare very quickly in some scenarios.[1]
On March 7, 2013, North Korea threatened the United States with a preemptive nuclear strike.[7] On April 9, North Korea urged foreigners to leave South Korea, stating that both countries were on the verge of nuclear war.[8]</td></tr>
<tr><td>Affected areas</td><td>A nuclear war would affect all areas – health, environment, economy, communications, transportations, etc.</td></tr>
<tr><td>Affected regions</td><td>The blast, heat, and radiation from a single nuclear weapon could kill hundreds of thousands of people in the region under attack. Depending on the scale of the nuclear war the entire population could be affected due to environmental consequences, including disruption of the Earth's climate and agricultural productivitiy.[1]</td></tr>
<tr><td>Affected domain</td><td>All domains could be affected.</td></tr>
<tr><td>Entry period
Application period</td><td>Until now the US remains the only country to have used nuclear weapons against another nation during the atomic bombings of Hiroshima and Nagasaki.</td></tr>
<tr><td>Empirical values</td><td>From 68,000 active weapons in 1985, there are now some 4,200 active nuclear warheads and some 17,000 total nuclear warheads in the world in 2013.[9] Many of the decommissioned weapons were simply stored or partially dismantled, not destroyed.[19]</td></tr>
<tr><td>Source</td><td>https://en.wikipedia.org/wiki/Nuclear_warfare.
http://www.ippnw.org/catastrophic-consequences.html.
http://www.ippnw.org/pdf/zero-is-the-only-option.pdf.</td></tr>
</table>

http://en.wikipedia.org/wiki/List_of_states_with_nuclear_weapons.
http://www.guardian.co.uk/world/2006/dec/12/germany.israel.
http://www.nytimes.com/2012/03/18/world/middleeast/iran-intelligence-crisis-showed-difficulty-of-assessing-nuclear-data.html?_r=0
http://www.reuters.com/article/2013/03/07/us-korea-north-attack-idUSBRE9260BR20130307.
http://www.cbc.ca/news/world/story/2013/04/09/north-korea-warning-evacuation-tensions.html.
http://www.fas.org/programs/ssp/nukes/nuclearweapons/nukestatus.html.
http://www.guardian.co.uk/news/datablog/2009/sep/06/nuclear-weapons-world-us-north-korea-russia-iran.

6.2.3 Environment

Title	**Air pollution**
Description	**Origin of threat:** manmade **Motives:** intentional **Methods/ Mode of actions:** Particulate air pollution is a mixture of solid, liquid, or solid and liquid particles suspended in the air. There are three principal air pollutants of major interest to agriculture: ***sulfur dioxide, fluorine compounds, and smog***. The last is a complex mixture of fog, carbon and dioxides. Over the last decades concentration of sulphur dioxide has decreased strikingly, ***attention has shifted to ozone, nitrogen dioxide, and particulates.*** **Impact:** Pollution, some visible, some invisible, that ***contribute to global warming***. Carbon dioxide, a greenhouse gas, is the main pollutant that is warming Earth. The major source of anthropogenic emissions of nitrogen oxides into the atmosphere is the combustion of fossil fuels from stationary sources (heating, power generation) and in motor vehicles. **Background:** The health effects of air pollution have been subject to intense study in recent years. Effects have been seen at very low levels of exposure and the key question is whether threshold concentrations exist below which air pollution has no effect on population health. If such a threshold could be identified, no additional public-health benefits would be expected from bringing air pollution concentrations far below this level. **Relevance in the future:** In addition to cohort studies on mortality, air pollution effects on morbidity endpoints have been studied. Most of these have been cross-sectional, and assume that current air pollution exposure is sufficiently representative of long-term, previous exposure to make a plausible link with current health status. Given the high cost of further measures to reduce air pollution, and the many new findings which suggest that health effects can be seen at ever lower concentrations, the health effects of air pollution will need to receive much scientific and regulatory interest for years to come
Affected areas	Urban and industry areas. Concentrations in city centers tend to be lower than those in suburbs, mainly as a result of the scavenging of ozone by nitric oxide originating from traffic.
Affected regions	Mostly in developed und industrialized countries
Affected domain	Environment
Entry period	
Application period	
Empirical values	Air Pollution Index (API) is a simple and generalized way to describe the air quality
Source	Brunekreef, Bert, et al., "Air pollution and health".

Title	**Water pollution**
Description	**Origin of threat**: manmade **Motives**: mostly unintentional **Methods/Mode of actions:** Water pollution is due to two different types of sources depending on the ways in which a pollutant gets an access to a water body. In case water pollution is from a single location as in case of a discharge pipe coming from a ***factory***, then it is termed as ***a point source of pollution***. Another example of this type can be in the form of an accidental spill from an ***oil tanker***. The place that is most affected by a point

	source of pollution is the area that is just next to the source of pollution. In case water pollution is due to multiple sources, then it is termed as **non point source of pollution**. In this case the pollutants are ultimately diverted into a water body (like fertilizers and pesticides). The human activities affect the quality of water in the water bodies. There are many **different causes of water pollution**:
	1. **Sewage**: Sewage waste poses a major problem. Sewage disposal leads to water borne diseases. The problem is quite acute in developing and under developed countries which do not have enough facilities for sewage treatment.
	2. **Agriculture**: Chemical fertilizers add nutrients to the soil but these nutrients ultimately drain into the rivers and oceans. The fertilizers along with the sewage dumped in the oceans can cause massive algal growth. This tends to remove oxygen from water and results in the creation of dead zones. Agricultural runoff also contains pesticides that find their way to underground water as well as rivers and oceans.
	3. **Industries**: Waste water resulting from manufacturing processes contains toxic chemicals. Large scale industries have suitable treatment facilities but small scale industries are unable to afford equipment required for pollution control.
	4. **Household activities**: All of us pour chemicals in the form of detergents used in dishwashers and washing machines into the drains. Eventually these end up in rivers and oceans.
	5. **Radioactive Waste**: The radioactive waste from nuclear power plants poses a great threat as the radiations given out from this waste may lead to cancer.
	Impact: Massive environmental damage. Water pollution may not only be a source of hindrance to activities like fishing but at the same time it may be hazardous to our health.
	Background: As a result of our day to day activities, we are adding those substances to water which do not actually belong to water. Massive investment in water technology enables rich nations to offset high stressor levels without remedying their underlying causes, whereas less wealthy nations remain vulnerable.
	Relevance in the Future: Potable water will become a rare commodity which will be difficult to afford. This development has already taken place in the most developing countries.
Affected areas	
Affected regions	Developing countries are the most affected regions, but it tends to get global
Affected domain	Environment, Nuclear
Entry period	
Application period	
Empirical values	About 80% of the world's population is exposed to high levels of threat to water security
Source	Global threats to human water security and river biodiversity, Nature 2010; ecorumors.com/2012/01/water-pollution-a-threat-to-life

Title	**Biodiversity loss**
Description	**Origin of threat**: manmade, natural hazards, climate change
	Motives: mostly unintentional
	Methods/Mode of actions: The main cause of the loss of biodiversity can be attributed to the influence of human beings on the world's ecosystem. In fact human beings have deeply altered the environment, and have modified the territory, exploiting the species directly, for example by fishing and hunting, changing the biogeochemical cycles and transferring species from one area to another of the Planet. The threats to biodiversity can be summarized in the following main points: **Alteration and loss of the habitats**; Overexploitation of resources; **Pollution, Introduction of exotic species and genetically modified organisms**; Climate Change.
	Impact: Many of the largest impacts of future biodiversity change on ecosystem services will arise from these shifts. Market cultivation leads to species and varietal specialization, threatening local diversity in land use patterns. If degradation continues, many of the region's most vulnerable peoples, in particular indigenous communities will be without a source of food, income, or habitat in which they have built their lives and traditions over the centuries.
	Biodiversity loss means loss of the insurance against habitat damage or species extinction. Relevant are diversity of species as well as races and sorts; inter and intra species diversity.
	Background: Habitat loss and degradation in terrestrial ecosystems cover a wide range of

	alteration of natural and semi natural ecosystems by human activities. Arguably, the conversion of forest to agricultural systems has been the most important of these habitat changes. Also because of reductions in river discharge from climate change and increasing water withdrawals, making a world that not only has fewer species but one that has fewer biotic differences among regions. Large biome shifts are very likely to occur. Aggressive climate mitigation substantially reduces species and biome range shifts. **Relevance in the Future:** Biodiversity support of ecosystem services as base for agriculture supported by the nature.
Affected areas	Habitats
Affected regions	
Affected domain	environment
Entry period	
Application period	
Empirical values	
Source	Intergovernmental Panel on Climate Change, "Climate Change and Biodiversity". Bovarnick, A., et al., "The Importance of Biodiversity and Ecosystems in Economic Growth and Equity in Latin America and the Caribbean: An economic valuation of eco-systems". Holsinger, Kent E., "Global Biodiversity Patterns". Lambin, Eric F., et al., "The causes of land-use and land-cover change: moving beyond the myths". Leadley, Paul, "CBD – Global Biodiversity Outlook 3. Scenario Synthesis". Pereira, Henrique M., et al., "Scenario for Global Biodiversity in the 21st Century". Sofian-Azirun, M. and Y. Norma-Rashid, "Biodiversity Conservation and Sustainable Use: Malaysian Scenario".

Title	**Complex nexus among resources scarcity: food, water, energy & minerals**
Description	**Origin of threat:** resource scarcity: manmade or caused by climate change **Motives:** intentional (manmade scarcity) or unintentional (caused by environment) **Methods/ Mode of actions:** Primary, resource scarcity is caused by *extreme resource exploitation on basis of rising consumption*. Stocks are declining rapidly over time without being able to recover. Short term scarcities can be observed by natural hazards as extreme weather conditions or climate change. Especially the *food production suffers* from this impact with crop losses *because of hail or droughts*. Also *market driven scarcities* are possible caused by trading food and minerals over the counter. This manmade scarcity is just the consequence of economic transactions. **Impact:** Resource scarcity will cause famines when food and water capacities are not enough or food is too expensive to afford for some people. Lacking of energy and resources to ensure a running infrastructure are consequences of scarcity which may lead to *economic decline*, and *less global resource exchange.* **Background:** The complex nexus among resources scarcity of food, water, energy and minerals based on key factors aggravating resource scarcity such as demographic trends, climate change, and expanding economic activities is difficult to understand. In turn, price volatility and supply shortages threaten to increase poverty, intensify hunger, trigger domestic and international conflict, and induce economic stagnation. Short term scarcity is not inevitably supposed to be naturally but more driven by economic development. **Relevance in the future:** It is important to realize the severity and complexity of resource scarcity in order to effectively addressing the scarcity challenges lying ahead. Making resource scarcity an extraordinary challenging issue by its far reaching global effects and the manner in which the four resources are connected. Global economic growth will continue to put pressure on a number of highly strategic resources, including energy, food, and water. This will increase the competition for the resources.
Affected areas	Political, economic, financial
Affected regions	All regions over the globe are affected from scarcity in a different way and intensity. Depending on the resource there is more or less demand in each country.
Affected domain	Environment
Entry period	Scarcity of resources have always been current during history
Application period	Scarcity is a permanent issue depending on the level of exploration and exploitation of demanded resources. Short term scarcity appears and disappears from time to time.
Empirical values	World market, stock exchange, energy exchange

Source	D.2.2

Title	**Deterioration or loss of ecosystem services**
Description	**Origin of threat**: mostly manmade but also natural **Motives**: mostly unintentional, trade-offs **Methods/Mode of actions:** Ecosystem services are the benefits people obtain from ecosystems. These include provisioning services such as food and water; regulating services such as flood and disease control; cultural services such as spiritual, recreational, and cultural benefits; and supporting services such as nutrient cycling that maintain the conditions for life on Earth. The problem posed by the growing demand for ecosystem services is compounded by ***increasingly serious degradation*** in the capability of ecosystems to provide these services. ***Examples***: World fisheries are now declining due to overfishing; agricultural land has been degraded in the past half-century by erosion, salinization, compaction, nutrient depletion, pollution and urbanization. Other human induced indirect impacts on ecosystems include alteration of the nitrogen, phosphorous, sulfur, and carbon cycles, causing acid rain, algal blooms, and fish kills in rivers and coastal waters, along with contributions to climate change. **Impact:** Human well-being is affected not just by gaps between ecosystem service supply and demand but also by the increased vulnerability of individuals, communities, and nations. Productive ecosystems, with their array of services, provide people and communities with resources and ***options they can use as insurance*** in the face of natural catastrophes or social unrests. While well-managed ***ecosystems reduce risks and vulnerability***, poorly managed systems can exacerbate them by increasing risks of flood, drought, crop failure, or disease. The cost of the loss of some ecosystem services could be very high. **Background:** Humanity has always depended on the services provided by the biosphere and its ecosystems. Further, the biosphere is itself the product of life on Earth. The composition of the atmosphere and soil, the cycling of elements through air and waterways, and many other ecological assets are all the result of living processes - and all are maintained and replenished by living ecosystems. The human species, while buffered against environmental immediacies by culture and technology, is ultimately fully dependent on the flow of ecosystem services. **Relevance in the Future:** There are many indications that human demands on ecosystems will grow still greater in the coming decades. Current estimates of 3 billion more people and a quadrupling of the world economy by 2050 imply a formidable increase in demand for and consumption of biological and physical resources, as well as escalating impacts on ecosystems and the services they provide. This combination of ever-growing demands being placed on increasingly degraded ecosystems seriously diminishes the prospects for sustainable development.
Affected areas	Ecosystem degradation tends to harm rural populations more directly than urban populations and has its most direct and strong impact on poor people.
Affected regions	Mainly forest areas and marine areas.
Affected domain	Environment
Entry period	Due to global demographic development, there can be expected that there will be an accelerating increase of potential deterioration or loss of ecosystem services.
Application period	There are no indicators for a decreasing demand of ecosystem services
Empirical values	
Source	United Nations Environment Programme (UNEP), "Global Environment Outlook 4". http://www.greenfacts.org/glossary/def/ecosystem-services.htm

Title	**Crime – Food Fraud and Food Terrorism**
Description	**Origin of threat:** man-made **Motives:** intentional **Methods:** Recent years have seen an increasing number of food safety incidents or 'food scares' (e.g. Melamine artificially boost apparent protein content in food, Clenbuterol residues in meat), which have received a considerable amount of attention in the media and have resulted in a decline in consumer trust. While this "Food Fraud" is not intended to harm people but rather to increase profit (e.g. Anheuser Busch being sued in the US for

	watering beer) "Food Terrorism" is defined as the deliberate contamination of the food or water supply. Foods can be used to spread chemical, biological or radionuclear agents. There are a wide variety of chemical agents that are potential weapons, including chemicals specifically developed for warfare (military), toxic industrial chemicals, and naturally-occurring chemicals such as ricin. **Impact:** The estimated and potential impact on human health can be Deliberate sabotage of food could have serious economic and trade repercussions. Industries in many sectors could be put out of business, and countries could experience severe economic and trade disruption. Many examples in the past prove that contamination of food and following worldwide re-calls can damage the economy of a country, dependent on the export of those goods, sustainably. **Background:** Terrorist attacks in the food supply would be difficult to distinguish from natural events, considering the large variety of human foodborne illnesses that occur every day, coupled with crop and livestock diseases. The International Food Standard IFS Version 6 requires that the responsibility for food defense in a company is clearly defined and documented. The requirements of the IFS are derived from U.S. authorities to ensure product protection and become binding for all companies seeking an IFS certification. **Relevance in the future:** According to the World Health Organization, food terrorism is "a real and current threat", with potential global health effects caused by an act of terrorism in one location. Large food production facilities with increasingly widespread distribution networks provide terrorists the avenue to insert agents that can render foods unfit for human consumption, cause harm to the population, and severely burden the economy.
Affected areas	This threat directly affects food and agricultural industry and the public health sector, but the greatest threat to the affected country is likely the economic impact of food terrorism.
Affected regions	Food fraud is not only linked to small-time criminals (Anheuser Busch being sued in the US for watering beer Largest brewer in the world – Budweiser, Michelob). In low-income countries or those with a limited range of exporting industries, the economic consequences of a terrorist act on food could also affect development and exacerbate poverty and even food availability.
Affected domain	Environment
Entry period	Any time, about to be considerably expanded
Application period	Food fraud and food terrorism are not necessarily new risk, but have always represented a threat. Some incidents have only recently been identified due to improved detection techniques. However, due to globalization and worldwide distribution of food the risk increased over the last years.
Empirical values	
weak signals	Deliberate release of a biological, chemical or physical agent, or radionuclear materials, could probably initially be considered as a natural or unintentional event.
Sources	Weak Signal Mining: WHO identifies foodborne disease outbreaks and incidents, including those arising from natural, accidental and deliberate contamination of food, as major global public health threats in the 21st Century. These threats require urgent action, and WHO recognizes that the building of global public health security rests on solid and transparent partnerships.

Title	**Plastic garbage patches as threat for food safety and security**
Description	**Origin of threat:** manmade **Motives: -** unintentional **Methods/ Mode of actions:** In the seas plastic waste is crushed by wave motion and UV light with an increasing degree of fineness up to pulverization. Various marine life including plankton tend to incorporate this plastic powder as food. These small particles often release toxic and cancer-causing chemicals such as polychlorinated biphenyls, bisphenol A and other chemicals, which can damage animals and finally reach the human food chain. **Impact:** Since 1980 there is an increasing amount of different plastics, visible on beaches and specific vortexes in the ocean. In the oceans these pieces of plastic form patches, caused by currents. Some of these very large scale patches have specific names, like the "Great Pacific Garbage Patch", which covers a remarkable part of the central North Pacific Ocean. The actual size is difficult to measure, because of the small size particles, but a size nearly twice the size of the US continent is discussed, based on estimation from sampling. There are other patches e.g. in the Indian and the Atlantic Ocean. At present,

	the impact to the human food chain cannot be quantified.
	Background: These patches are characterized by high concentrations of pelagic plastics, chemical sludge and other debris that have been trapped by the currents. Despite its size and density, the patch is not visible from satellite photography, since it consists primarily of suspended particles in the upper water column. These concentrations of submerged particles are not visible from space, nor do they appear as a continuous debris field. Instead, the patch is defined as an area in which the mass of plastic debris in the upper water column is significantly higher than average.
	Relevance in the future: Despite the fact, that there are some efforts to reduce plastic waste in oceans, there is no evidence that the actual amount of plastic did decrease up to. Rather, it is not unlikely, that there will be an increasing amount of very small plastic particles and chemicals from plastic in the human food chain in the long run. As consequence there is some research need to deal with these long term consequences of very small plastic particles in the human food chain.
Affected areas	This threat affects environmental research, biological research, food security and Safety as well as waste research and is relevant for the plastic and chemical industry, food industry, especially sea food production and the corresponding value chain.
Affected regions	In general, all regions in the world are potentially affected, but particular regions with sea food production and consumption will be affected.
Affected domain	Environment
Entry period	As the plastic waste is the main source of this threat and the process from waste production to environmental contamination and biological absorption is very long, it can be expected, that there is a slow but steady increase of potential damage.
Application period	The awareness of effects on the human food chain is increasing; however it is not easy to quantify real effects. In Austria, there is a recommendation of the Ministry of Health for pregnant women not to eat fish, because of high bispheno A values. It can be expected that the potential for a negative effect s on food safety of garbage patches will increase, at least in the next 10-20 years, as the water in the large-scale ocean circulation needs years for a full circulation. The long run scenario will depend on effective plastic waste management.
Empirical values	Only for size and trend of the plastic garbage patches in the seas and not for consequences on food safety.
weak signals	Plastic waste on beaches, in the sea and the increasing tendency to smaller particles. Plastic particles in marine life. Levels of Bisphenol A and other toxic or carcinogenic substances in sea food.
Sources	Weak Signal Mining

Title	**Greenhouse effect / Global warming**
Description	**Origin of threat**: manmade
	Motives: unintentional
	Methods/Mode of actions: The greenhouse effect helps to regulate the temperature of our planet. It is essential for life on Earth and is one of Earth's natural processes. It is the result of heat absorption by certain gases in the atmosphere (called greenhouse gases because they effectively 'trap' heat in the lower atmosphere) and re-radiation downward of some of that heat. Water vapor is the most abundant greenhouse gas, followed by carbon dioxide and other trace gases. Without a natural greenhouse effect, the temperature of the Earth would be about -18°C instead of its present 14°C. So, the concern is not with the fact that we have a greenhouse effect, but whether ***human activities are leading to an enhancement of the greenhouse effect*** by the emission of greenhouse gases through ***fossil fuel combustion and deforestation***. Human activity has been increasing the concentration of greenhouse gases in the atmosphere (mostly carbon dioxide from combustion of coal, oil, and gas; plus a few other trace gases).
	Impact: Increasing heat content in the ocean is consistent with ***sea level rise***, which is occurring mostly as a result of thermal expansion of the ocean water as it warms. Global mean sea level has been rising at an average rate of 1.7 mm/year over the past 100 years, which is significantly larger than the rate averaged over the last several thousand years. However, this increase is due mainly to thermal expansion and contributions from melting alpine glaciers, and does not include any potential contributions from melting ice sheets in Greenland or Antarctica (see also Relevance in the Future)
	Background: Global surface temperatures have increased about 0.74°C since the late–19th century, and the linear trend for the past 50 years of 0.13°C per decade is nearly

	twice that for the past 100 years. The warming has not been globally uniform. Some areas (including parts of the southeastern U.S. and parts of the North Atlantic) have, in fact, cooled slightly over the last century. The recent warmth has been greatest over North America and Eurasia between 40 and 70°N. **Relevance in the Future**: The land areas will warm much faster than ocean temperatures, particularly those land areas in northern high latitudes (and mostly in the cold season). Additionally, it is very likely that *heat waves and other hot extremes will increase*. *Precipitation is also expected to increase* over the 21st century, particularly at northern mid-high latitudes. Over mid-continental areas *summer-drying is expected* due to increased evaporation with increased temperatures, resulting in an increased tendency for drought in those regions. *Snow extent and sea-ice* are also projected to decrease further in the northern hemisphere
Affected areas	The whole ecosystem
Affected regions	Developing countries are the most affected regions, but it tends to get global.
Affected domain	Environment
Entry period	
Application period	
Empirical values	Pre-industrial levels of carbon dioxide (prior to the start of the Industrial Revolution) were about 280 parts per million by volume (ppmv), and current levels are greater than 380 ppmv and increasing at a rate of 1.9 ppm yr^{-1} since 2000. The global concentration of CO_2 in our atmosphere today far exceeds the natural range over the last 650,000 years of 180 to 300 ppmv. According to the IPCC Special Report on Emission Scenarios (SRES), by the end of the 21st century, we could expect to see carbon dioxide concentrations of anywhere from 490 to 1260 ppm (75-350% above the pre-industrial concentration). The Electricity Sector is responsible for about one third of European GHG emissions, Households and Services generate 15 percent, the Transport Sector produces 20 percent, the Waste Sector produces 3 percent and the Agricultural Sector is responsible for 10 percent.
Source	GHG Mitigation in the EU: An Overview of current Policy Landscape, World resources Institute 2012; National Climatic Data Center 2013

Title	**Growing western dependency on oil, gas and import of minerals and high tech metals**
Description	**Origin of threat:** manmade **Motives:** intentional **Methods/ Mode of actions:** The dependency on oil, gas and import of minerals and high tech metals continues. These are *highly needed resources which cannot be self assured in the western states*. There are efforts to develop alternative sources of energy before maximum global oil and gas production will be exceeded, however it is unclear, if the renewable energy sources completely substitute the conventional energy plants. **Impact:** Having no overarching alternative to these minerals will *trigger high oil price* and *erosion of support for environmental protections*, leading to widespread development of whatever energy sources are most available, regardless of the long-term consequences. This also makes the West *vulnerable to any instability in the Middle Eastern* oil producing countries. **Background:** Since the industrial revolution there is a need for minerals as input for generating energy. The share of fuel and energy exports in hard currency revenues reached its highest level. In the 1980s, the economy was tuned to the needs of the extracting sector in general and the oil and gas sector in particular. While in Soviet times there were reasons to speak of mineral extracting sectors – particularly oil and gas extraction – as a burden on the economy, analysts now tend to speak of the oil and gas sector as a locomotive promoting economic growth. **Relevance in the future:** Despite efforts to develop alternative sources of energy, oil consumption is still rising rapidly, what is likely to continue for the next 25 years. It may happen that in the future Europe will be an "active outsider".
Affected areas	This threat affects the industry especially the highly energy based industry. Further on households, travel and transportation
Affected regions	Western countries and particularly even the EU
Affected domain	Environment
Entry period	Current period and remains up to date until the renewable energy power stations can be regarded as a competitive alternative.

Application period	Dramatic climax of dependency when delivering countries are running out of raw materials.
Empirical values	
Source	D.2.2

Title	**Habitat loss and degradation – forest and coral reefs as an example**
Description	**Origin of threat**: manmade, climate change, natural hazards **Motives**: unintentional **Methods/Mode of actions:** Habitat loss and degradation in terrestrial ecosystems cover a wide range of alteration of natural and semi natural ecosystems by human activities. Although natural events such as landslides and earthquakes do alter the landscape, they generally occur in isolated areas and healthy ecosystems are able to recover from them. *Human-caused habitat loss*, on the other hand, is altering ecosystems on a global scale, often causing destruction that is irreversible, at least on a time scale that is of interest to society. The *conversion of forest to agricultural systems* has been the most important of these habitat changes. Further reasons are a *not appropriate planting* (no local tree species) or expansion of *species-poor plantations*. Forest degradation *caused by fires* becomes a problem when they burn in the wrong places, or at the wrong frequency or the wrong temperatures. Globally, most forest fires are probably now directly or indirectly influenced by humans. *Natural-caused habitat loss* due to the climate change is projected to cause major *changes in marine habitats*, through increased water temperature, ocean acidification, and expansion of oxygen minimum zones. *Tropical corals are vulnerable* to climate change because increases in sea surface temperature of 1°C for more than 8 weeks can lead to strong coral bleaching. In addition, ocean acidification reduces the availability of carbonate for calcification, slowing the growth of corals, and along with bleaching and other stressors, **Impact:** Habitat loss and degradation causes a loss of biodiversity, a loss of ecosystem services and therefore a deterioration of human well-being. *Fires* can alter the structure and composition of forests, opening up areas to invasion by fast-colonizing alien species and threatening biological diversity. Effects could be: Buildings, crops and plantations are destroyed and lives can be lost; Destruction of assets for companies; For communities: loss of an important resource base, impacts on water cycles, soil fertility and biodiversity; For farmers, fire may mean the loss of crops or even livelihoods. *Vulnerability of corals* leads to widespread degradation of coral reefs and the ecosystem services they provide such as fisheries, storm surge protection, and income from tourism. **Background**: Deforestation and degradation of forests create ecological problems in every part of the world. Deforestation is occurring at a rapid pace, especially in tropical regions where millions of acres are clear cut every year. Remaining forests also suffer from pollution and selective logging operations that degrade the integrity of local ecosystems. **Relevance in the Future**: Eliminating all deforestation is not possible. Parts of the landscape will need to be reshaped and altered as populations grow and change.
Affected areas	See Impact
Affected regions	Mainly forest areas and marine areas.
Affected domain	Environment
Entry period	
Application period	
Empirical values	Further deforestation and continuation of global warming.
Source	Bovarnick, A., et al., "The Importance of Biodiversity and Ecosystems in Economic Growth and Equity in Latin America and the Caribbean: An economic valuation of ecosystems". Pereira, Henrique M., et al., "Scenarios for Global Biodiversity in the 21st Century".

Title	**Introduction of invasive alien species**
Description	**Origin of threat**: manmade, climate change **Motives**: intentional and unintentional

	Methods/Mode of actions: Alien species are animals, plants and micro-organisms that spread or are introduced to areas beyond their natural geographic range due to human activities. Alien species may be ***introduced to new areas deliberately or unintentionally*** through activities such as cargo shipping. Alien species are considered to be "invasive" when they present a risk of harm to the environment, economy and/or human health of the new areas that they inhabit. Invasive alien species being introduced to ecosystems to which they are not adapted i.e. where they have no, or not enough, predators, to maintain an ecological balance. The introduction of invasive species is certainly facilitated, if not ***caused, by the level of international transport and traffic of goods of our trade system.*** **Impact:** Invasive species are one of the ***primary threats to biodiversity***. It is estimated that invasive species contributed to nearly 40 % of all animal extinctions for which the cause is known since the 17th century. Invasive species may exert ***negative impacts on an ecosystem by***: • competing for food, water, space, and other resources; • altering the habitat; preying directly on or parasitizing native species; • weakening the gene pool by interbreeding with native species; and • spreading disease (an invasive species may also be a disease itself). **Background**: Biological invasions by alien (cf. non-native, non-indigenous, foreign, and exotic) species are recognized as a significant component of global environmental change, often resulting in a significant loss in the economic value, biological diversity and function of invaded ecosystems. Numerous alien species, many introduced only in the last 200 years ago, have become successfully established over large areas of Europe. In the late 1990s increasing awareness of the impact of biological invasions in Europe arose from clear evidence of impacts reported in regional environmental audits. By 1998, the Community Biodiversity Strategy identified invasive alien species as an emerging issue of environmental importance and in March 2002, the European Council recognized that the introduction of invasive alien species was one of the main recorded causes of biodiversity loss and the cause of serious damage to economy and health. **Relevance in the Future**: Invasive species have been identified as "a main direct driver of biodiversity loss across the globe." Current trends suggest that the rate and risk of introduction of invasive species have increased significantly in recent years as it will continue. Future global biodiversity scenarios highlight potentially dramatic increases in biological invasions in European ecosystems. Interacting effects through rising atmospheric CO_2 concentrations, warmer temperatures, greater nitrogen deposition, altered disturbance regimes and increased habitat fragmentation may facilitate further invasions.
Affected areas	There are no specific areas.
Affected regions	There are no specific regions.
Affected domain	Environment
Entry period	Historically, invasive alien species issues have relatively low visibility in the European Community, outside specialist circles. However, in the late 1990s increasing awareness of the impact of biological invasions in Europe arose from clear evidence of impacts reported in regional environmental audits. By 1998, the Community Biodiversity Strategy identified invasive alien species as an emerging issue of environmental importance and in March 2002, the European Council recognized that the introduction of invasive alien species was one of the main recorded causes of biodiversity loss and the cause of serious damage to economy and health.
Application period	
Empirical values	In the United States, the cost of biological invasions has been estimated to total $97 billion hitherto for 79 major bioinvasions. Although only limited monetary data are available at present for Europe, there is a similar indication that biological invasions have imposed losses on the economy. The strongest evidence is for alien pest and weeds that impact upon the agriculture, forestry, aquaculture and other sectors.
Source	Institute for European Environmental Policy (IEEP), "Scenarios and models for exploring future trends of biodiversity and ecosystem services changes". http://www.ecoissues.ca/index.php/Trends_in_invasive_alien_species. Hulme, Philip E., David Roy, Teresa Cunha and Tor-Björn Larsson, "A pan-European inventory of alien species: rationale, implementation and implications for managing biological invasions".

Title	**Loss of arable land**
Description	**Origin of threat**: manmade, natural hazards, climate change

	Motives: mostly unintentional, trade-off **Methods/Mode of actions:** Arable land is any land that can be used to grow crops. Many of the practices used in growing these crops can lead to the ***loss of topsoil and soil characteristics*** that make agriculture possible. The loss of arable land has been caused by a number of factors, many or most of which are tied to human development. The primary causes are ***deforestation, overexploitation for fuel wood, overgrazing, agricultural activities*** and ***industrialization***. Also ***urban-sprawl is in conflict with arable land***. Soil sealing is higher due to the increased land consumption for building. **Impact:** When agriculture fields replace natural vegetation, topsoil is exposed and can dry out. The diversity and quantity of microorganisms that help to keep the soil fertile can decrease, and nutrients may wash out. Soil can be blown away by the winds or washed away by rains. This can cause clogged and polluted waterways and increased flooding and causing declines in fish and other species. The shrinking of arable land and the massive land degradation threatens the ***ability of the country to maintain current levels of agricultural production***, while the widening gap between rural and urban is an important challenge to the right to food of the global population. **Background**: Farm and ranch land is desirable for building because it tends to be flat, well drained and affordable. Over the past 20 years, the average acreage per person for new housing almost doubled with best agricultural soils being developed the fastest. The sprawl in industrialization and urbanization affects agricultural land leading to its scarcity. This change in turn definitely affects the socio-economic conditions. Thus, the existing land use/ land cover pattern, changes in land use pattern and the relationship between population growth and food production is a matter of major concern. **Relevance in the Future**: Continued loss of arable land will endanger our ability to feed the world population. Land degradation is worldwide - both developed and developing countries. Restoration is very problematical.
Affected areas	The health of soil is a primary concern to farmers and the global community whose livelihoods depend on well managed agriculture
Affected regions	All regions where there is agricultural activity. Middle and East Europe is an area of particular local concern.
Affected domain	Environment
Entry period	
Application period	
Empirical values	
Source	http://worldwildlife.org/threats/soil-erosion-and-degradation, http://www.globalchange.umich.edu/globalchange2/current/lectures/land_deg/land_deg.html, http://peakwater.org/tag/loss-of-arable-land/

Title	**"Natech" disasters (Natural disasters in combination with man-made accidents)**
Description	**Origin of threat:** natural influence and manmade **Motives:** (un)-unintentional **Methods/ Mode of actions:** Disaster researchers and emergency management responders have traditionally classified disasters as either natural or technological. "Natech" disasters are a ***combination of technological failures and environmental processes*** (e.g. natech-disaster is the total meltdown in Chernobyl) or can rather be natural events or catastrophes that in turn cause technological and industrial failures. Natech disasters represent nowadays key concerns of security research. **Impact:** Technological disasters often leave the "built" and "modified" environments intact, but severely, and oftentimes permanently, contaminate the "biophysical environment". In contrast to natural disasters, technological disasters result in more severe long-term social and mental health impacts for survivors. In fact, the impacts of natech disasters, similar to technological disasters, are often masked by latent ***health risks due to toxic exposure*** and slowly evolving patterns of collective stress, anger, anxiety and depression. **Background:** The complex causality of disasters and their crosscutting nature is why it became increasingly difficult for agencies to respond effectively referring to technological and/or natural disasters. In general natural disasters cause loss of life and destroy infrastructures. The risks and dangers, which are caused by natural disasters in urban areas, are intensified due to a variety of interconnected risk elements. Increased vulnerability to natural disasters gives reason to develop a reliable forecast in order to

	prepare for natural hazards. Diversifying the risk of natech disasters only work by reducing or prevent technological failures. **Relevance in the future:** The relevance of this issue for the EU is increasing due to intensifying land use, industrial and infrastructure development, urban expansion and the proximity of populations to industrial sites. Within highly networked and technologically reliant society, unlikely events with massive consequences, will actually become more likely and will occur more frequently over the coming decades.
Affected areas	Security research
Affected regions	This is a global threat. But studies could find out most of (natural) disasters occur in urban or transition zones.
Affected domain	Environment
Entry period	
Application period	"Natech" disasters increase with technology development/ application
Empirical values	An example for a natech-disaster is the total meltdown in Chernobyl. Generally there is an increased trend for the named types of hazards. Also, 86% of the disaster events occurred in urban or transition zones, whereby urban spaces ranging from 20 000 to 100 000 inhabitants received the most impacts (data out of over 67 000 disaster events in eight countries in Latino America)
Source	D.2.2

Title	**Pharmaceutical residues from pharmaceutical discharges or residues of veterinary drugs**
Description	**Origin of threat:** man-made **Motives:** unintentional **Methods:** The demographic trend towards ageing populations in many countries is resulting in marked increases in the quantity and diversity of pharmaceuticals and their metabolites released into the environment. The quantity of veterinary medicines required to support increases in food production for a growing human population is also expected to rise. Increasing wealth and economic development in many parts of the world, coupled with ready availability of lowcost generic pharmaceuticals, also are likely to increase drug use and subsequent discharge. Furthermore pharmaceuticals may enter the human food chain as residues due to administration to livestock.. **Impact:** Early concerns regarding pharmaceuticals in the environment focused on the feminisation of fish by components of oral contraceptives. More recently, the presence of antibiotics in freshwater and coastal environments has been linked to the spread of antibiotic resistance. An increasing range of pharmaceuticals is currently detectable in the environment. These include statins, anti-hypertensives and cancer chemotherapy agents, reflecting treatments administered to an increasing number of people over 50 years of age. The effects on non-human species of increasing concentrations of current and new pharmaceuticals (e.g. nanomedicines), particularly in complex mixtures, have yet to be assessed. Not only the direct uptake of pharmaceutically active residues, e.g. as Clenbuterol used as anabolic in meat production, is of major concern but also the selection of resistant bacteria in the gastrointestinal tract and disruption of the colonization barrier of the resident intestinal microflora due to constant uptake of antibiotics with food **Background:** The occurrence and fate of pharmaceutically active compounds in the aquatic environment has been recognized as one of the emerging issues in environmental chemistry. In some investigations carried out in Austria, Brazil, Canada, Croatia, England, Germany, Greece, Italy, Spain, Switzerland, The Netherlands, and the U.S., more than 80 compounds, pharmaceuticals and several drug metabolites, have been detected in the aquatic environment. Several pharmaceutically active compounds from various prescription classes have been found at concentrations up to the μg/l-level in sewage influent and effluent samples and also in several surface waters located downstream from municipal sewage treatment plants. **Relevance in the future:** In general, it has been believed that the environmental concentrations of active pharmaceutical ingredients are too low to constitute a risk to human health in developed countries, and several studies have been conducted to assess

	this perspective. However, a recent poll among expert stakeholders reported that 62% of those interviewed believed that pharmaceutically active compounds in the environment represent a risk to human health. As the global population ages, the use of pharmaceuticals to alleviate age-related conditions can reasonably be expected to increase. Further, the ongoing development of large markets such as China and India will further increase the magnitude of pharmaceutical consumption. In recent years, higher potential exposure levels to pharmaceutically active compounds in the environment in developing countries, potable water reuse and public health concerns regarding antibiotic resistance are receiving increased attention.
Affected areas	This threat affects the environmental research, biological and agricultural research, food security and safety as well as human health. Intensified multidisciplinary studies between medical, food and environmental sectors may give more insight on effects in the future.
Affected regions	In general all regions in the world are potentially affected, but particular regions with further increase of pharmaceutical consumption, but mostly regions with poor sewage treatment or control of veterinary drugs.
Affected domain	Environment, food and agricultural industry, public health system
Entry period	Anytime, but with an increase within the next 10-20 years
Application period	Already the awareness of possible effects on environment or human health is increasing and a lot of studies on environmental effects are undertaken. At the same time food analysis includes the detection of drug residues. But the control of medication strongly depends on policy and inspection.
Empirical values	Clenbuterol can be used as an example for incidents in the past. Clenbuterol is a bronchodilator used in asthma medicine worldwide for the treatment of allergic respiratory disease in horses. A common trade name is Ventipulmin, and it can be used both orally and intravenously. Clenbuterol is also a non-steroidal anabolic and metabolism accelerator, through a mechanism not well understood, which is why it is used illegally by athletes to build muscle. Its ability, however, to induce weight gain and ensure a greater proportion of muscle makes its illegal use in livestock popular. Clenbuterol accelerates the catabolism of fat in pigs and, when added to feed, it not only shortens growth time but also increases the sale price of pork and pig organs. Meat containing clenbuterol often has a bright red skin with very little fat. However, approval in the EU is for bovine and equidae use only. In February 2009, 70 people fell ill after eating pork products contaminated with clenbuterol. The victims, all in Guangdong province, consumed meat bought from markets in Guangzhou, the provincial capital of Guangdong, which came from farms in the neighbouring Hunan province. Since 1998, there have been at least 19 clenbuterol food poisoning cases in China affecting more than 1,750 people including one confirmed death.
weak signals	Increased anti-biotic resistance, increased abnormities in fauna and flora, decreased fertility rates, levels of pharmaceutical residues in foodstuffs
Sources	Weak Signal Mining: Various sources e.g. Williams, E.S.; Brooks, B.W. Human Health Risk Assessment for Pharmaceuticals in the Environment: Existing Practice, Uncertainty, and Future Directions; Human Pharmaceuticals in the Environment; Emerging Topics in Ecotoxicology Volume 4, 2012, pp 167-224; ISBN 978-1-4614-3419-1

Title	**Resource access triggered conflicts within and between states**
Description	**Origin of threat:** manmade conflict **Motives:** intentional conflicts **Methods/Mode of actions:** Within the next fifty years the planet's human population will probably pass nine billion and global economic output may quintuple. There will be *conflicts due to a lack of resources and an increasing rate of exploitation*. **Impact:** This is a global threat. Scarcity of resources makes people fight to get access to highly needed goods/ valuable resources. *Developing countries are expected to suffer* most because of the greater dependence from the developed countries. However, due to globalization, advanced societies will be also affected. Rising energy prices on the world market and mounting concerns about environmental depletion have animated fears that the *world may be headed for a spate of "resource wars"*. **Background:** Basic needs such as *water and food supply* are most important to assured nutrition for living. A lack of access to these resources may end up in conflicts within and between states. During history, states often took advantage of their power to conquer resource wealth areas in order to ensure their stock of natural important resources. For

	instance in 1867 Alaska became another state of the USA to ensure several oil deposits. **Relevance in the future:** In the future world conflicts will be triggered by climate change and resource scarcity. Especially water wars and conflicts about access to energy sources will occur in the future. Political instability and conflicts in the energy producer countries will be one consequence. Perceptions of scarcities of resources will drive countries and domestic groups to assure their future supply. There is the rise of China which is accompanied with the use of many resources such as oil, gas, timber and most minerals. Further on the depletion of resources in developing countries and the global climate change, which could multiply stresses on natural resources and trigger water wars, are the most important drivers for conflicts.
Affected areas	The global factors social wealth and consumption behavior may be affected as well as EU policy, R&D and economy.
Affected regions	Climate change affects the world globally. In the area of Kashmir, water wars are very probable. Central Asia has already become an area of international competition for access to energy. Referring to the energy producer countries, i.e. Iran, Iraq and Libya are threatened.
Affected domain	environment
Entry period	Currently existent in several regions in the world
Application period	The awareness of rarely use of resources and sense for environmental issues gets increasingly important and is not supposed to fade in the future
Empirical values	Empirical values referring to climate change are raising temperature and greenhouse gases. "Resource wars" have always been a part in our history.
Source	D.2.2

6.3 Interviews with stakeholders Phase 2

We want to make it very clear, that some of the statements of the interview partners are facts and many others are personal opinions. These opinions sometimes differ widely between interview partners and do not necessarily represent the opinion of the consortium.

6.3.1 Cyber infrastructure

In this chapter the results of six completed interviews in the area of cyber infrastructure are summarised.

6.3.1.1 Threats

One interviewee stated that the **complexity of systems** is increasing and with it the potential to misuse the system. The IT market is constantly changing with many new systems on the market.

A mayor threat is seen in the **lack of education of the end-user**. The end-users are not aware of the security risks of commercial products like computers, smartphones or tablets. The commercial products are not configured well and the end-users do not care about a proper configuration of the systems, like fire-walls, virus-scanner or software updates. Especially small businesses buy branded equipment, but do not spend much effort on configuration.

The **increase of mobile devices** is also seen as a threat. Smartphones are used for payments; they contain personal data like identity cards or are used for check-in at airports. The problem arises when people agree on a standard, e.g. the security risks of pcs started when Microsoft Windows became a standard. Today we experience the same with Android and Apple iOS. The security risks of these two systems will increase massively. In this area baseband attacks will be a critical factor. Often systems are put on the market as soon as they are "acceptably solid". Their vulnerability however at this stage is often high.

Furthermore, in most cases security measures are attached afterwards and are not considered from the start of the product development. In the IT domain people are still not used to security measures, whereas when driving a car it is has become natural to use a seat-belt. Another interviewee also sees a lack of design or manufacturing (e.g. in robots) as a threat.

It is also seen as a problem by one of the interviewees that the providers often make use of so-called 2nd or 3rd line contracts. It is not always clear whether these systems contain bugs or "backdoors" (see the Huawei case for an example[4]).

Potential vulnerabilities are also situated with a number of vital utility companies, in the area of finance, energy and telecom. In the event of potential misuse, the greatest impact can be felt here.

Another interviewee sees the main threat in the **usage of SCADA** (supervisory control and data acquisition) as an industrial control system. The problem is that the life cycle of these machines are very long (around 20 years), so that the computers who are working with these machines

---

4   William Wan and Craig Timberg, China slams congressional charges against its telecom firms Huawei and
     ZTE, Washington Post, 9. Oct. 2012.

renew very slowly. But the main problem is the lack of awareness. The people working with these machines do not realize that they have a security problem; therefore the security in these machines often lags 10 years behind the state-of-the-art. The companies want to get remote access to their automation processes and are using "toys" like tablet PCs. The tablets are not designed to control industrial processes or even nuclear plants.

EC-cards and credit cards don't provide the latest security standards. But at the moment the damage is still minor, so that the banks do not bother to introduce safer systems. Presently the damage is paid by the banks or insurance companies, so that the clients do not withdraw themselves in online banking.

One interviewee said that in the area of cyber threats there are several players. There are still single hackers. But at the moment there is a huge shift in this area. Today behind these hackers are big organizations with a lot of money. For example there are organisations in South America, who formerly have been active in the area of human trafficking or drug dealing, are now working in cybercrime, which is quite lucrative. Nowadays, cyber-criminals seem to be more motivated by a desire to gain financially than to cause electronic vandalism.

One interviewee mentioned the computer worm **Stuxnet**, which most probably had the aim to stop the uranium enrichment infrastructure in Iran. It was mentioned that this attack created the pressure in the "community" to replicate this capacity.

Cyber-war is much cheaper than conventional warfare. With the amount of money necessary to buy a bomber there could be caused a far bigger damage in the cyber domain. One interviewee sees the challenge that the trust put in consumer devices/services will be hampered, if these devices are misused (e.g. security breach at DigiNotar, a Dutch certificate authority[5]).

The lack of trust of the consumers has also impact on the economy. The consumers start to be aware of the effects of their own actions (e.g. no security updates) and start to withdraw themselves from the market and don't use the newest and best technologies – e.g. they decide not to use smart phones anymore. The consequence is that companies get in trouble.

One interviewee sees a threat in general security responses, such as ID cards, and the way that identity security flaws could make things worse. Sometimes security policy introduced into technology can increase the risk of security (e.g. smart meters). Policy makers act with one agenda in mind (e.g. deploy smart meters) and rarely think about second order effects in the drive to implement the policy. Additionally, an increasing potential for "movements" (good but also bad ones) in societies is observed, that is strongly supported by social media.

Development of threats and hazards in the next 5 years

The interviewees were also asked on their views on how the threats and risks will develop during next 5 years.

In general the interviewees found this question rather hard to answer. It is not easy to see if the current dynamics will change and will lead to increased awareness and more secure platforms. Generally the interviewees assume that **cyber-crime and cyber-espionage will increase** and

---

5   Wikipedia, DigiNotar, http://en.wikipedia.org/wiki/DigiNotar, seen at 23. Jan. 2013.

will be even more sophisticated in the future. While some interview partners are more optimistic and think that we will generally overcome the security risks, so that even if there are more limitations and boundaries in cyber space, for the end-user there won't be a lot of changes. Other interview partners believe that we will face a big cyber crash within the next 5 years.

One interviewee is observing that the amount of crime rises every 6 month by 300%. Both the gravity of the threats as well as the costs of the incidents is growing fast. They think that within 3 years we will reach a **global peak in IT-usages**. From then on the disadvantages of the internet will outweigh the advantages and the users will start to withdraw themselves from the internet. At the moment the internet is not capable of adapting - for example the prosecution of cyber criminals is not working well.

6.3.1.2   Societal needs

The interviewees saw the following points as crucial for the societal need:

- We need education and awareness. The people should be educated in internet security from play school age onwards.
- We need a forum for discussions. Policy makers should talk to companies. We have to establish a dialogue between all stakeholders, so that we can develop standardisations and a healthy system in the future.
- There should be international, mandatory rules. At the moment we have "best practices", but this is not working. Thus we need tools to enforce these rules. Freedom should still be the basis of the internet – but there also should be rules, so that internet will not die. It was suggested that it should be mandatory for all companies to have an insurance against the risks of cybercrime. This way the companies would be forced to invest in their security to get the insurance. They would use systems which are secure by design. Adjustments to the design of systems based on risk analysis can seriously reduce the exposure to cyber threats.
- We need security by design. In new ICT systems vulnerabilities should be limited from the very beginning.
- The companies should disclose when they were breached. Firstly, because then the experts of cyber security would know what is going on and secondly the business world should know when a company is breached (e.g. when intellectual property was stolen).
- In many organizations the people responsible for cyber security do not have enough access to decision-maker level. Those responsible for taking the decision as to whether or not purchase a particular system should be made more aware of the potential vulnerabilities with respect to cyber security, both on governmental as well as on a private sector level.

6.3.1.3   Solutions

One of the interviewees said that it is of key importance to form institutional structures at the international level. It is important to create a **level playing field of institutions**, so that people/organizations can exchange information at the same level and with similar mandates. The Computer Emergency Response (CER) teams or national cyber security centres in each country have different structures and mandates. If we want to make sure that vulnerabilities are better addressed, particularly cross-border, this will have to be harmonized. **International agreements** like the ones for road traffic should be implemented. We need governmental regulations, so that research and industry are forced to develop security solutions (e.g. airbags also haven't been introduced by themselves).

The **transparency of the cyber systems** should be improved. At the moment there are too many competing security systems. We need standardised security systems and a collaborating industry – no lobbying. We need policies which lead to less fragmented security systems.

It was stated that it is important that we have to follow **international standards** and that we use hardware with **build-in security**. Rigorous testing of technologies is also seen as important. Randomised controlled trials might be helpful, but systems tend to get properly attacked when they are out in the wild being fully in use. One expert sees the particular need for a European infrastructural network with a **high level of redundancy** (excess capacity, the ability to fall back on additional capacity when a disruption occurs).

One interviewee said that it is not necessary to develop new technical solutions. The problem is that the people are unaware of how many technical solutions already exist in the area of cyber security. We should **educate the engineers** how to create safe software. At the moment in many cases the engineers are not aware how to do it. We also need processes for handling security risks without human interference (like anti-lock brakes in cars). The **end-users should be aware** if they have a misconfigured PC or if there credit card number was stolen. At the moment it is possible to blame the manufacturer or the bank issuing the credit card. The problem is that the end-users do not get feed-back about their errors. One interviewee thinks that in **high-security areas** we should go for our own national products.

A main problem is seen in user authentication. We need **proper user authentication** so that we can prove that someone is innocent or has been committing cybercrime. The interviewee claimed that today with a good lawyer you can always say that the log-files were forged. Another interviewee said that we need harder ways of going after the technology producers and holding them accountable. We need to be able to get answers from Google or Microsoft regarding the question what they are doing to make their devices secure.

It was also said that the debate about security within the companies or in governmental agencies is dominated by the marketing voice – but we should increase the **engineering risk perspective**. The expert advocates Science and Technology studies for all policymakers. The other way round scientists and researchers should be trained in political communications.

6.3.1.4 Secondary effects of security solutions

There is the challenge to find a balance between freedom and security. The security should have high standards, so that we have low risks. If we have too many regulations, hackers will be motivated to find a way around it and organizations like Anonymous will then start to cause problems. If millions of people in Facebook get angry about security regulations, the society will also get a problem. Another interviewee thinks that it is more a problem of security on the one side and tremendous investments (financial limits) on the other side. However, if vulnerabilities are tackled head-on, the consumer faith in the stability of applications/ devices/ services will grow. This could represent a business opportunity in itself.

The privacy question is relevant to mobile applications. Can the end-user trust that the data is secure? The responsibility for privacy issues lies primarily with the product developer, but the government can of course take on an active role. One interviewee said that all security solutions could also be used for evil purposes –e.g. Intel-AMT (active management technology). The system uses two processors – one processor contains the operating systems and the second processor is still running after the user has shut-down the system. This way IT service provider are able to reconfigure the BIOS or to remotely manage the system. Due to the same feature Intel-AMT is something like a super-backdoor to the system.

6.3.2 Nuclear

In this chapter the results of six completed interviews in the area of nuclear material are summarised.

6.3.2.1 Threats

In general nuclear threats and challenges are divided into three categories – state actors, non-state actors and accidents.

State Actors – Nuclear Proliferation

One important threat is seen in **nuclear weapon arsenals**. The nuclear countries have resisted and stalled in the process to get rid of their nuclear arsenal and have continued to elevate the status of nuclear weapons in their own security policy. There are agreements (e.g. US-Russia) to reduce the arsenals, but these are not really dedicated efforts to reduce all military nuclear materials and weapons.[6] This in turn has been a contributing factor to the desire of other countries to acquire nuclear weapons. Unless there is a mechanism that involves everybody in this process, old suspicions and misunderstandings are frozen.

There are many ways in which nuclear weapons pose a problem. The most extreme end is a **nuclear war** due to accident, miscalculation, an error prone command and control, "broken arrow", etc. Nobody expects that to happen, but the arsenals are maintained at those levels. A single use against a city is regarded to be more plausible. It could be a decision out of desperation in critical regions.

Presently there are 5 nuclear weapon states (United States, Russia, United Kingdom, France, and China), 3 non-NPT[7] nuclear powers (India, Pakistan, North Korea) and one undeclared nuclear power (Israel). Apart from these states Iran is working intensely on the development of technologies to improve centrifuges. If Iran had a nuclear weapon, that would be a threat to the world order. A North Korean nuclear weapon is also very dangerous - an instable region North Korea/ South Korea would also affect the rest of the world.

Plutonium is generally well protected, but interested states might obtain it by exploiting unburnt mixed oxide (MOX) fuels. Plutonium as well as enriched uranium is also available in civil research reactors. Spent nuclear fuel cannot generally been used to produce nuclear weapons, but if this material is separated in nuclear reprocessing plants it gets more dangerous.

In the military domain there are approximately several hundred tonnes of weapon-grade uranium, e.g. in independent states of the former Soviet Union, in the US and other nuclear weapon states. An interview partner stated that for one nuclear weapon an amount of 6 to 10 kg uranium would be sufficient. In all these military institutions there are people working who might potentially steal nuclear material.

---

6   There is a new initiative of President Obama:
     http://www.regjeringen.no/en/dep/ud/press/news/2013/nuclear_initiativ.html?id=730950

7   Non-Proliferation Treaty (NPT)

Terrorist Attacks – Dirty bombs

Material for **dirty bombs** can be obtained from many sites. It is hard to prevent the theft of small amounts of radioactive material, e.g. from research laboratories. The security arrangements in research laboratories are generally very high, but it is still possible to steal small amounts. However, it is discussed theoretically if this type of terrorism is attractive to terrorists at all.

The security of existing material is a general issue - it includes weapons as well as civilian material (e.g. radioactive waste of nuclear power plants, radioactive sources from hospitals or material inspectors). In the military domain (without counting nuclear power) there are globally transfers of tens of tonnes of material. The sheer number creates the possibility of some material being misplaced, lost or stolen. One interviewee said that in the non-civilian domain each country does it best to protect its material, but there is no clear picture of how good these efforts are.

There is also seen a potential threat in a **terrorist attack on a nuclear site**. For example, terrorists could threaten to attack these sites with conventional weapons or using cyber-attacks. The IT systems of nuclear power plants in Europe vary widely. At the moment there are no specific indications of an imminent attack. But it is assumed that we have to be generally prepared against an attack driven by cultural or religious backgrounds. There are international agreements that set out some responsibility; e.g. there are conventions for physical protection and a convention against terrorism etc. The basic problem is that these impose very few specific obligations on physical protection. The only legally binding obligation is to protect civil material in international transports. Everything else is up to the individual countries.

On the last nuclear security summit in Seoul (2012) the participants especially discussed measures to combat the threat of nuclear terrorism, the protection of nuclear materials and the prevention of illicit trafficking of nuclear materials. Especially the area of civil radioactive sources is a broad field, as the practices of the different users differ significantly.

Nuclear power plants – accidents:

Apart from terrorist attacks on nuclear sites also **accidents at power plants** could have serious consequences, especially in Europe with its dense populations.

Fukushima could happen anywhere in Europe. In Western Europe people usually argue that the power plants have containments, but in Eastern European countries there are still plants without containment.

Development of threats and hazards in the next 15 to 20 years

The interviewees were also asked for their opinion on how the nuclear threat will develop in the next 25 to 20 years.

One interviewee said that there are different directions. On the one hand the nuclear weapons states have modernization plans. Although the US and Russia are reducing the numbers of nuclear weapons, they are only getting rid of the old ones and are investing in new generation designs and missions. If this continues it will be very difficult to stop other countries from starting their own nuclear weapons programme. Another expert also expects that the risk of proliferation will increase. He thinks that apart from Iran there will be other countries who will strive for nuclear weapons. On the other hand there are growing groups of non-nuclear states in

and outside the Nuclear Proliferation Treaty (NPT), who have a new interest in the humanitarian consequences of nuclear weapons.

In the area of state-actors there aren't expected any radical changes; there probably will be a slow progress. One interviewee hopes that there will be a progress in the development of institutional arrangements for disarmament that could help reduce the distrust in the system. That in turn would help build better relationships and would have a positive effect on nuclear disarmament. Another expert thinks that it is generally difficult to foresee the developments in the nuclear domain within the next 20 years. Especially the area of nuclear terrorism is hard to predict. Probably there will be new technical threats and new weapon developments. For instance, nobody could foresee in the 70s or 90s that there might be suicide bombers like in 9/11. Previously people thought that the nuclear waste would protect itself, because of the high radiation. Today we have to think differently.

6.3.2.2   Societal needs

The interviewees saw the following points as crucial for the societal need:

- Protection of citizens from exposure to nuclear material and radiation
- Prevention of accidents (e.g. at nuclear sites)
- Prevention or reduction of nuclear proliferation
- Protection from nuclear weapons

The events (e.g. accidents, terrorist activities, nuclear war) all have a low probability but a high impact. Therefore we need a **good crisis management** to be prepared for the case of a release of radioactivity. Apart from a strategy how to react to an event, we need better detection technologies and personnel with specialist knowledge. Police and fire service have to be better prepared for a nuclear event.

Both nuclear weapons and nuclear power plants left the society with the enormous burden of toxic and radioactive material. The society should make **deep strategic and political shifts** and instead of maintaining nuclear arsenals, the states should make investments to deal with urgent issues like climate change, food and water resources shortages as well as clean and sustainable energy sources.

One interviewee thinks that Europe can't afford an accident like Fukushima, due to which we would have to give up a region in Europe. His consequence is the **withdrawal from the nuclear energy** programme. Apart from that he thinks that we need to upgrade the security in existing nuclear power plants and to improve police work in this domain.

One of the interviewees thinks that the organisations and institutions involved in maintaining nuclear capabilities are all fairly strong and that these institutions need more **public attention and control**. The public should make sure that the discussions on nuclear material are not dominated by vested interests.

Another interviewee sees the need that the **government should make clear and easy to understand statements.** At the moment the society has a widespread mistrust of governmental institutions and prefers to believe in "experts" which have high media attention. In case of the implementation of new security standards or specifically in case of emergency it is important for the government to have the trust and comprehension of the citizens.

6.3.2.3   Solutions

In the area of **nuclear weapons** the interviewees see a necessity to improve the verification and technical monitoring system of the Non Proliferation Treaty (NPT). The monitoring and inspection systems of the treaty are in a much better state now, but they still need to be improved. Essential are also confidence building measures among the states.

One interviewee said that on a technical level a proper system for the **dismantling and disposal of nuclear weapon** materials is needed. They have to be secured and kept in an environmentally responsible way. It was also suggested to spend additional research funds in the area of "safe disarmament" and into the handling and storage of nuclear weapon materials. Another interviewee believes that there is no technical solution for the problem of the misuse of nuclear material. All the technical attempts (like alternate fuels for nuclear power plants or surveillance systems) only give a false feeling of security. To make progress in the area of nuclear disarmament and the security of nuclear material the only way is seen in **cooperation** – in working institutional structures, exchange of information and inspection of sites.

We also need new ways of **counter-terrorism**. We have to put ourselves in the position of the terrorist to learn how they are thinking.

We also have to improve **reactor safety** – are our power grids safe enough for nuclear power plants? We also have to think of **final disposal sites** for nuclear waste – a best possible solution has to be found.

There is also a need for better **detection systems**, e.g. for border control.

6.3.2.4   Secondary effects of security solutions

One interviewee said that the supporters of nuclear weapons always mention that nuclear weapons work well as a deterrence and therefore contributes to stability. But in his opinion our species should grow up and solve the underlying conflicts and problems without falling back on war and violence.

Another interviewee mentioned that for example in nuclear sites a lot of security measures are implemented which all have data protection & privacy aspects. People have to hand over their identity cards as well as mobile phones. They are searched and everywhere inside the building there are video cameras. The interviewee thinks that it is crucial that the persons affected are well informed about why and how the security measurements are implemented.

6.3.3   Environment

This chapter contains the combined results of eight interviews in the area of environmental issues.

6.3.3.1   Threats

In general the interviewees observe that the threats in the area of environment are getting more complex.

Interviewee 1	Interviewee 2
Hurricanes	Flooding
Storm surge	Avalanches
Flooding	Other natural disasters
Snow drifts (collapsing roofs due to the snow load)	Power blackout
Heat waves (water scarcity)	Pandemics
Interruptions of supply change	Accidents releasing radioactivity (Fukushima)
Oil leakages (on the coast)	
CBRN accidents or attacks	
Earthquakes (especially in Istanbul)	
Tsunami in the Mediterranean	
Impact of natural hazards on critical infrastructure	

Table 13: Important threats and hazards mentioned by the interviewees

One of the threats most frequently mentioned by the interviewees is **climate change**. The climate change has quite different impacts on different countries and regions. In general it affects most of all the poorest regions of the world – in these regions it could intensify already existing conflicts (e.g. ethnic or religious motivated conflicts) and in the end this could lead to the collapse of the society.

Impacts of climate change in a ten years perspective is not a big threat, but after that it will be. Risks associated with climate change are new migration patterns. Another risk is that climate change could increase imbalances within the EU, especially between the North and the South. Climate change is also seen as the driver for a series of consequences like sea-level rise, glaciers melt, crop shortfalls, change of Gulf Stream, spread of tropical diseases, loss of biodiversity, migration, and so on.

Flooding is also seen as an important threat to society. There have been a number of great flood defence projects, but this is coming under increased financial constraint.

Another important issue is seen in the **efficient use of resources**. We have built our economy and our society on the inefficient use of natural resources (e.g. energy) and now we are seeing the secondary effects of that usage. For example, there has been a debate about "peak oil" for a while and now we are starting to see that other resources like phosphorus also might have a "peak". This is also related to the concept of planetary boundaries. Historically, the access to natural resources has been many times a trigger for conflicts.

One interviewee said that our society is especially vulnerable in the area of **agriculture**. Thus for example **water scarcity** would be a particularly hard hit. Water scarcity would also have an effect on price development and the food industry. These effects will ultimately most badly effect the poor population. This again causes risks of instability.

The **loss of biodiversity** will also have consequences for the human beings. It will probably take some time until we will feel the consequences of the loss of biodiversity –our ecosystem is quite robust. But at some time in the future we will see the signs. Religious motivated interviewees added that we are asked to cultivate and preserve the creation.

Ethical principles are also the reason to take a more sceptical attitude towards **genetically modified crops**. Another technological area about which we know little regarding its societal long term effects is **nanotechnology**.

Another high system level hazard is seen in EU politics which aims to appropriate the resources of poor countries (e.g. **land grabbing or biofuels**). One interviewee sees a threat in the

commercialisation of the ecosystem. Although ecosystem services are an important concept that might be part of a solution regarding environmental problems, but there are also risks if we put "a price on the environment".

Environmental pollution can occur in various forms: **water-, air-, soil- and sound pollution**. If dangers arise to public health, this is often at a local level. In large parts of the world this can lead to potential social unrest. Large scale environmental pollution can lead to diseases and/or to soil pollution/degradation which reduces the arable land. One Interviewee sees a big threat in **chemical accidents,** both inside industrial companies as well as during transport of hazardous materials. The expert is worried about a situation getting out of hands, if a hazardous material is widely spread and a large number of persons have to be evacuated.
Another expert is especially worried about environmental pollution due to excess unreacted nitrogen compounds entering the environment. In the agriculture we are using multiple times the amount of **nitrogen** naturally introduced to the soil. Additionally we have the problem of excess nitrogen compounds in waste water.

An important issue is the **non-point pollution** (e.g. if you add fertiliser, not all of it is taken up by the plant, thus excess nutrient will leave the cultivation area and enter ground/surfaces water; unlike a normal point source – like a pipe – a cultivation area is a non-point pollution). The increasing dead areas in the Gulf of Mexico and off coast of China originate mainly from non-point sources.

Beside the fact that our oceans are being depleted of **fish stock** (e.g. places near Newfoundland, where there is simply no more life in the sea), a growing phenomenon is so-called "plastic-soup". Fish eat plastic material, which causes the fish to die. The plastic material at times also makes its way in the food chain. We still have an insufficient overview on the impact of this specific threat to public health.

There are some historical cases and there are also theoretical calculations, which indicate that **solar storms** could be a serious threat to modern society.

Development of threats and hazards in the next 15 to 20 years

One interviewee thinks that perhaps in Northwest Europe and the US and perhaps even in China the society will have enough innovative capacity to **adapt sufficiently to the pace of developments** (population growth, need for energy, food and water). But many less developed countries and regions in the world will face difficulties. Another interviewee also thinks that in the next 15 to 20 years Europe will not undergo serious societal changes due to environmental threats. On the other side in poorer regions of the world, the climate change will probably lead to famine in this period of time.

The interviewees assume that due to the **climate change** threats like flooding or heat waves, but also secondary effects like power blackouts will be more frequent than today.

It is also assumed that the **scarcity of resources** will get worse. Especially fossil resources will become scarce (peak oil theory). A lack of available water supplies, the lack of nutrients like phosphates and therefore food insecurity can lead to tremendous **price volatility with respect to natural resources** and water. This volatility will potentially lead to migration flows, social unrest and socio-political instability.

6.3.3.2   Societal needs

Within the European Union there is a need to **spread the knowledge** about climate change and its consequences. The society should develop a deeper understanding of the underlying problem. Additionally the society should be **educated** how to live with the consequences of climate change - how to behave in hot summers and how to protect themselves in flood areas. It is more difficult to educate the society outside Europe, as every small region might have its own problems regarding climate change. So it is necessary to provide all the specific information for this local area and include also the traditional knowledge of the local people. The problem is that in many cases the local population does not have the (financial) resources to accomplish the adaption process to climate change on its own. In these cases they have to rely on international help.

The interviewees agree that it is also very important to raise **awareness and understanding in the society** that the government is not able to solve all kind of problems. The society and each individual have to make their own preventions (personal responsibility) – e.g. some water and food storage to be prepared for the case of a power blackout.

Another important need is **prevention**. This is for example possible due to standardization (e.g. standards for construction, so that the roofs do not collapse under the snow load). But also in general we have to be better prepared to deal with emergencies and crisis. We need to start developing social norms about change, that help us to adapt more rapidly in ways that help us to mitigate the crises and emergencies.

We have to enhance the **social acceptance of necessary decisions**. The fundamental problems will not be solved without some sacrifice. We have to transfer the insight into politics, so that voters will actually vote for it. The question is if people are willing to accept solutions/policies that might lower the standard of living in conventional terms.

One interviewee also sees a need in **better communication** to be able to cope with the problems ahead. There is a need to enhance communication between different groups in society, groups that are not very active in interactive dialogue today (e.g. "people in the field" and researchers, government and commercial sector).

Corruption is also seen as a huge problem. In order to mitigate threats we must fight corruption. We also need better understanding of what corruption really is and how it could be mitigated.

6.3.3.3   Solutions

Several interviewees mentioned that we should promote the **resilience** of the society. We should provide trainings and programmes so that the people are better able to help themselves in case of an emergency. Also **knowledge and education** about climate change are seen as key issues. We should learn more about **decision science**, what motivates people, what makes people change. It is not sufficient to have the technological solutions; we also have to understand what makes people accept the change (e.g. incandescent light bulbs in EU; difference of energy consumption in EU and USA).

We also need better **warning systems**. At the moment we do not have a good warning system to be able to evacuate a city of one million people. One interviewee suggests intensifying research in the area of the usage of smart phones as part of the warning system. It is also seen as important to promote international **networks** of experts and end-users and to make sure that

these networks are not dominated by national views. We should also try to cooperate outside the "comfort zone", i.e. do not only cooperate with likeminded western nations. One interviewee said that we need better capabilities in the area of **logistics** and infrastructure (energy, telecommunication, water, administration). For example we should be able to provide the citizens with an extensive electricity supply in case of an emergency. Another important area is **communication**. We should be able to sustain at least the communication of the crisis management team (authorities, civil defence, military) in a scenario with a power blackout of several days.

We should invest in **better capabilities in the area of reconnaissance**, search and rescue of people as well as technologies for indoor localization and transmission of vital signs. **Energy issues** were mentioned by several interviewees as key to sustainability and security. An important part is the energy turnaround to include more renewable energies in our system as well as research in better energy storage technologies.

One of the interviewees said that it would be very helpful if plants and food crops would grow with less water and energy. That would make our **food system** more resilient. It will also be of great value, if we manage to convert seawater into drinking water at a low cost and a lower energy usage. **Gene technology and nanotechnology** are seen as promising areas by one of the interviewees. It was said that these technologies should be pursued to help us solve our problems.

6.3.3.4 Secondary effects of security solutions

The interviewees mentioned that the following security solutions might have secondary effects:

- Genetically modified plants
- Nuclear energy
- Biofuel
- Carbon capture and storage (CSS)
- Fracking
- Data protection & privacy (e.g. are civil defence personal allowed to track mobile phones of people who might be submerged?)
- A more energy way of life will probably lead to a reduction of the range of different life-styles (houses, cars)
- Less population growth (there are some people who think that the population should always grow)
- Change of the energy prize structure (When the prize of gasoline rises, the value of large used cars will decrease. If poor people can only afford to buy a car that is fuel inefficient, they will be less able to travel or to find work. Thus equity issues will arouse and this will happen globally.)

6.3.4 Context

There are also threats related for the context. These threats are described in the following chapters.

6.3.4.1 Threats

Terrorism in general continues to be a significant threat to society – in particular in crowded places. There is some evidence that people are aware of the danger, but the longer we go

without an event occurring, we become more complacent. The danger is that we become less security conscious and don't do the right things when events occur.

The greatest threat to security is seen in an **incremental change in the way that people look at traditional politics** and the way it can meet their needs. Particularly among young people, this goes hand in hand with the growth of social media, globalisation, and interconnectivity of people and the diversity of societies. When a shock comes into the system ways of voicing the anxieties are needed. When traditional politics are not seen as the answer, shocks can sometimes spill over into violence (e.g. English riots, rise of "golden dawn" in Greece).

Unemployment and inequality like the **growing gap between the "haves" and the "have nots"** are seen as threats. The financial crisis has a big impact in this area. Social instability is seen as a hot topic. This is based on increasing socioeconomic differences as well as on a lack of trust between people and between citizens and authorities.

Policy makers have a tendency to think about terrorism, counter-terrorism, laws etc. and are missing the point that **politics is alienating key parts of society** (e.g. people are conflating militancy with Islamic militancy and see Muslims as "the threat").

The **increased polarisation** is considered as one important threat which embraces different levels, e.g. the increase of political parties who are against immigration as well as immigrants who lack trust in society and feel reluctant towards integration.

Another, but related threat is that **large groups are not part of society**. They don't go to school, they don't work, they don't get (don't want) economic support from society. These people are not taking part in society's systems, which increase their alienation and make them more susceptible to extreme movements, e.g. criminal gangs, extremists, etc.

It is a problem that **people from different groups do not meet each other**. There are too few places where people from different cultural and/or ethnic groups meet.

The debate about energy security is dominated by the issue of finite resources. At the moment the focus lies exclusively on costs – the **security of supply** is not considered. The deregulation of critical infrastructures in society has not been good and it has been made without adequate risk analysis. The deregulation has presupposed that the marked based economy system is functioning, but the marked based principles emanate from peaceful conditions and they are not able to manage stress.

Infrastructure failure is a problem due to financial constraints. Because of the economic downturn we can see failures to maintain road and rail infrastructure.

Another interviewee sees the **ageing critical infrastructure** as a threat. Negative effects on infrastructure are especially the case when the temperature passes through zero degrees Celsius. Society is not well prepared for a large breakdown of critical infrastructures and especially long power failures are considered as a real threat. At the moment, attention is particularly paid to the transport systems, but almost no discussion is held on water and sewage systems.

One problem when discussing threats is that low probability/high consequences scenarios tend to attract almost all the attention. However, this is not what costs most to society.

6.3.4.2   Societal needs

The interviewees saw the following points as crucial for the societal need:

- In some countries individualism is very strong and the family is relatively weak, as is civil society. We must find other ways beside the private sector, the public sector and the individual. The civil sector must play a larger role. These actors are more trustworthy in some eyes compared to the state.
- There is a need to preserve the basic services that are related to a Welfare State to manage security issues. Changes regarding to public services and living standards can be a conflict driver in Europe.
- We have to learn how to manage conflicts without violence. We have to manage increased diversity as well as increasing economic austerity, lack of jobs, etc.
- We need to address the gap of a lack of mechanism for voice. We need platforms so that those practitioners (peace building organisations, community workers), who have traditionally worked to support capacities of communities to deal with conflict, have a voice that is linked to policy.
- We need a better integration of the emergency services across Europe. The interoperability need to be improved, particularly in relation to terrorism and major events.
- The terrorist threats are shifting down to lower levels where they are harder to predict and detect. Thus for the necessary prevention capacity we need to invest continuously in security services and the police.
- We also need new and innovative methods of reminding the public, so that people remain vigilant.
- We need to learn more about the psychology of emergency services (particularly in dealing with terrorism).
- We have to develop cooperation between various actors in areas that are cross-sectorial (e.g. cyber and energy security). We also have to analyse the flows and dependencies regarding for instance energy supply.

6.3.4.3   Solutions

The interviewees saw the following points as crucial for solutions:

- In some countries individualism is very strong and the family is relatively weak, as is civil society. We must find other ways beside the private sector, the public sector and the individual. The civil sector must play a larger role. These actors are more trustworthy in some eyes compared to the state.
- Regarding cyber and energy security we need national strategies. In both areas several sensitive and difficult questions needs to be addressed. Regarding cyber, these include which systems ought to be protected and if we should have an offensive capacity.
- We should develop better definitions of what ought to be protected in society and what vulnerabilities the society has.
- There is a need to improve transparency regarding access to risk data and to the current trends of threats in order to inform the population. This issue is critical and it needs to be done carefully, because the communication of risk data can also create fear among the population – people can feel insecure.
- Another issue is to invest in voluntary people; for instance the significant role of voluntary fire fighters.

6.4 Weak Signals Mining – classification of weak signals

Nr	Title of weak signal	Domain	Source	Threat/ opportu-nity	Social need	Potential for wild card
1	Stuxnet as first SCADA attack software platform	Nuclear, Environment, Cyber	TIA	x	x	7
2	Advanced persistent threats (APT), like Ghostnet	Nuclear, Environment, Cyber	TIA	x	x	6
3	Black Market prices explosion of Zero day exploits	Cyber	TIA	x	x	8
4	Military cyber attack unites	Nuclear, Environment, Cyber	TIA	x	x	9
5	Modular botnet development platforms	Cyber	TIA	x	x	6
6	Trojan horse software service industry	Cyber	TIA	x	x	6
7	Globalisation, strategic sourcing and cloud services	Cyber	TIA	x	x	8
8	Global advertising networks and private data exchange	Cyber	TIA	x	x	10
9	Dark nets and cryptographic peer to peer nets for anonymous publishing and whistle blowing	Cyber	TIA	x	x	9
10	Global black hacker industry and black markets	Cyber	TIA	x	x	7
11	Epistemic networks for knowledge exchange in organised crime	Cyber	TIA	x	0	7
12	Surprising side effects of genetic engineering	Environment	TIA	x	0	10
13	Nuclear terrorist attack	Nuclear	TIA	x	0	8
14	Nuclear espionage of non state actors	Nuclear	TIA	x	0	8
15	Uncontrolled release of nuclear waste	Nuclear	TIA	x	0	8
16	Dirty Bombs and CBRN terrorism	Nuclear	TIA	x	0	8
17	Water pollution and peak water	Environment	TIA	x	0	9
18	Air pollution without boarders	Environment	TIA	x	0	7
19	Land pollution with human waste	Environment	TIA	x	0	7
20	Noise pollution on land and sea	Environment	TIA	x	0	6
21	Light pollution in industrialised countries	Environment	TIA	x	0	5
22	Deforestation, loss of biodiversity and desertification	Environment	TIA	x	0	9
23	Plastic garbage patches in the ocean	Environment	TIA	x	0	7
24	Globalisation of food fraud	Environment	TIA	x	0	8
25	Collapse of space waste	Environment	TIA	x	0	10
26	Systemic risk: Takeover of virtual currency supplier, by organised crime	Cyber	TIA	x	0	10
27	Acidification of the ocean	Environment	TIA	x	0	10
28	Agro-terrorism	Environment	TIA	x	0	10
29	A new power on the horizon - Global virtual communities	Nuclear, Environment, Cyber	TIA	x	x	10
31	The Shadow of the Bomb: The Risks of WMD Proliferation and Terrorism	Nuclear, Environment	Sigma Scan	x	0	6
31	Eco-Terrorism: A Rising Threat?	Environment	Sigma Scan	x	0	4
32	Living With Terror: Democracy and Terrorism	Nuclear, Environment, Cyber	Sigma Scan	x	x	9
33	A Society of Surveillance?: The National Introduction of ID Cards?	Cyber	Sigma Scan	x	x	1

34	Defining Paths: The Shape of Islam in the 21st Century	Nuclear, Environment, Cyber	Sigma Scan	x	x	8
35	One Flag, Many Nations: The Establishment of an International Army?	Nuclear, Environment, Cyber	Sigma Scan	x	x	9
36	Will We Have Armies in the Future? Declining Recruitment Rates for the Armed Forces	Nuclear, Environment, Cyber	Sigma Scan	x	x	9
37	Globalisation: Could the Barriers be Going up Again?	Nuclear, Environment, Cyber	Sigma Scan	x	x	5
38	Globalised Migration: Complex Human Transfers	Environment,	Sigma Scan	x	x	2
39	Return to the Ark	Environment,	Sigma Scan	x	0	2
40	Bio-Breakout: A World Swept by Pandemics	Nuclear, Environment, Cyber	Sigma Scan	x	0	5
41	Saving Lives Through Disaster Prediction	Nuclear, Environment, Cyber	Sigma Scan	0	x	2
42	Protecting Air Quality: The Effects of Air Pollution in Developed and Developing Countries	Environment,	Sigma Scan	x	x	1
43	Quenching the Thirst: International Water Shortages?	Environment,	Sigma Scan	x	x	4
44	All the World is a Stage: The Increasing Power of Transnational Corporations	Nuclear, Environment, Cyber	Sigma Scan	x	x	5
45	Inclusive Security?: United Nations Security Council Enlargement?	Nuclear, Environment, Cyber	Sigma Scan	0	x	1
46	Public Service, Private Provider?: Future Implications of the Growth of PFI Schemes	Nuclear, Environment, Cyber	Sigma Scan	0	x	1
47	Serious, Organized and Networked Crime: Criminal Networks in the era of Globalisation	Nuclear, Environment, Cyber	Sigma Scan	x	0	9
48	Raising the Stakes: Will Iran Develop Nuclear Capability?	Nuclear	Sigma Scan	x	0	3
49	A Modern Icarus: Could Solar Flares Cause Communication Meltdown?	Nuclear, Environment, Cyber	Sigma Scan	x	x	6
50	Who's Looking at you? Increasing Mass Surveillance	Nuclear, Environment, Cyber	Sigma Scan	x	x	7
51	Plenty More Fish in the Sea?: The Depletion of Fish Stocks.	Environment	Sigma Scan	x	x	5
52	Sowing a Bitter Crop: Global Reductions in Available Arable Land	Environment	Sigma Scan	x	x	6
53	To Arms: The Growing use of Lethal Force in Violent Crime Across Europe	Nuclear, Environment, Cyber	Sigma Scan	x	x	5
54	Talking Rubbish: The Struggle to Conquer the Growing Waste Mountain	Nuclear, Environment	Sigma Scan	x	x	8
55	The Kraken Awakes: the Impact of a Cataclysmic Seismic Event	Environment	Sigma Scan	x	0	10
56	End-game?: A Major Asteroid Impact on Earth	Environment	Sigma Scan	x	0	10
57	Gene Out of the Bottle: Could Genes from GMOs Proliferate in Nature?	Environment	Sigma Scan	x	0	10

58	Virtually Criminal: the Rise of Internet Crime	Cyber	Sigma Scan	x	x	8
59	The Oil Crisis: Any Light at the End of the Pipeline?	Environment	Sigma Scan	x	x	9
60	Geoshifts in Innovation	Nuclear, Environment, Cyber	Sigma Scan	x	0	9
61	Sensors and Tracking: Finding Anything, Anywhere, Anytime	Cyber	Sigma Scan	x	x	8
62	Security: Marrying Technological and Human Approaches	Cyber	Sigma Scan	x	x	3
63	Who's in Charge: Choosing, Funding and Communicating Science Projects	Nuclear, Environment, Cyber	Sigma Scan	0	x	2
64	Understanding Complexity: How to Answer the Big Questions	Nuclear, Environment, Cyber	Sigma Scan	x	x	1
65	A Droid for All Seasons: Robots Become More Versatile	Nuclear, Environment, Cyber	Sigma Scan	x	x	7
66	Synthetic Chemical Cells – A New Way for the Invention, Discovery, Synthesis and Production of Molecules and Materials	Environment	Sigma Scan	x	x	6
67	Surviving Peak Oil	Nuclear, Environment, Cyber	Sigma Scan	x	x	10
68	Nuclear NIMBY: Meeting the Challenges of Next-Generation Nuclear Waste Management and Public Acceptability	Nuclear	Sigma Scan	x	x	6
69	Continued Growth in Energy Consumption	Nuclear, Environment	Sigma Scan	x	x	8
70	Dangerous Climate Change and Tipping Points	Nuclear, Environment, Cyber	Sigma Scan	x	0	10

Table 14: List of weak signals with classification as threat/ opportunity, need or wild card

Nr	Weak Signal	Domain	Potential for wild card	Comment
1	Stuxnet as first SCADA attack software platform	Nuclear, Environment, Cyber	7	Disruptive innovation with potential long term consequences
2	Advanced persistent threats (APT), like Ghostnet	Nuclear, Environment, Cyber	6	Disruptive innovation with potential long term consequences
3	Black Market prices explosion of Zero day exploits	Cyber	8	Possible long term trend, with a potential for additional disruptive events.
4	Military cyber attack unites	Nuclear, Environment, Cyber	9	Structural change in military strategy
5	Modular botnet development platforms	Cyber	6	Disruptive innovation with potential long term consequences
6	Trojan horse software service industry	Cyber	6	Disruptive innovation with potential long term consequences
7	Globalisation, strategic sourcing and cloud services	Cyber	8	Disruptive innovation with potential long term consequences and disruptive events
8	Global advertising networks and private data exchange	Cyber	10	Disruptive innovation trend with a potential for dramatic loss of privacy

9	Dark nets and cryptographic peer to peer nets for anonymous publishing and whistleblowing	Cyber	9	Disruptive innovation trend with a potential for dramatic loss of secrecy
10	Global black hacker industry and black markets	Cyber	7	Possible long term trend, with a potential for additional disruptive events.
11	Epistemic networks for knowledge exchange in organised crime	Cyber	7	Possible long term trend, with a potential for additional disruptive events.
12	Surprising side effects of genetic engineering	Environment	10	GMOs in the wild, might have a high impact in the evolutionary balance, **similar to 55**
13	Nuclear terrorist attack	Nuclear	8	Disruptive event with long term consequences
14	Nuclear espionage of non state actors	Nuclear	8	Preparation for nuclear terrorist attack
15	Uncontrolled release of nuclear waste	Nuclear	8	Disruptive event with impact on long term trend in life span.
16	Dirty Bombs and CBRN terrorism	Nuclear	8	Disruptive event with long term consequences
17	Water pollution and peak water	Environment	9	Long term trend, but with tipping points as a potential for violent disruptive events in specific regions.
18	Air pollution without boarders	Environment	7	Global long term trend, with a potential for future conflicts.
19	Land pollution with human waste	Environment	7	Regional long term trend, but with a potential for disruptive events.
20	Noise pollution on land and sea	Environment	6	General trend in industrialized countries, and a specific problem, e.g. with sonar
21	Light pollution in industrialised countries	Environment	5	General trend in metropolitan areas
22	Deforestation, loss of biodiversity and desertification	Environment	9	Long term trend, but with tipping points a potential for disruptive events.
23	Plastic garbage patches in the ocean	Environment	7	Long term trend, but with a potential for long term impact.
24	Globalisation of food fraud	Environment	8	Long term trend, but with a potential for disruptive events.
25	Collapse of space waste	Environment	10	Long term trend, but with a global break down of satellite infrastructure as specific tipping point.
26	Systemic risk: Takeover of virtual currency supplier, by organised crime	Cyber	10	Widely unrecognized potential for a large scale break down of the currency system.
27	Acidification of the ocean	Environment	10	Long term trend, but with a high potential for disruptive events, similar to climate change.
28	Agro-terrorism	Environment	10	Similar to biological or entomological warfare, but with non state actors. Can have a long time impact on the environment
29	A new power on the horizon - Global virtual communities	Nuclear, Environment, Cyber	10	
31	The Shadow of the Bomb: The Risks of WMD Proliferation and Terrorism	Nuclear, Environment	6	9/11 already, was a game changer, the next large scale attack will just lead to improvements
31	Eco-Terrorism: A Rising Threat?	Environment	9	As sabotage, no game changer, but with weapons from biological warfare a possible disruptive event, **similar to 28**
32	Living With Terror: Democracy	Nuclear,	9	The 'war on terror' is likely to change

	and Terrorism	Environment, Cyber		shape from direct military intervention towards counter-terrorism and intelligence-gathering, and will rely more on communication and persuasion. Thus, structural change of military
33	A Society of Surveillance?: The National Introduction of ID Cards?	Cyber	1	No game changer
34	Defining Paths: The Shape of Islam in the 21st Century	Nuclear, Environment, Cyber	8	Democracy in countries where Islam is in the ascendant, will probably be very different to that current practiced in Europe or North America.
35	One Flag, Many Nations: The Establishment of an International Army?	Nuclear, Environment, Cyber	9	Structural change in army (Globalisation), **similar to 32**
36	Will We Have Armies in the Future? Declining Recruitment Rates for the Armed Forces	Nuclear, Environment, Cyber	9	Structural change in army(recruitment), **similar to 32**
37	Globalisation: Could the Barriers be Going up Again?	Nuclear, Environment, Cyber	5	Globalisation is a well known long term driver for changes
38	Globalised Migration: Complex Human Transfers	Environment,	2	Migration is well known
39	Return to the Ark	Environment,	2	No game changer, but long term trend
40	Bio-Breakout: A World Swept by Pandemics	Nuclear, Environment, Cyber	5	Last global breakout in 1920 was not a game changer
41	Saving Lives Through Disaster Prediction	Nuclear, Environment, Cyber	2	Long term trend in innovation
42	Protecting Air Quality: The Effects of Air Pollution in Developed and Developing Countries	Environment,	1	No game changer, but long term trend in some countries
43	Quenching the Thirst: International Water Shortages?	Environment,	4	Maybe a game changer in the future, but it is an expected long term trend
44	All the World is a Stage: The Increasing Power of Transnational Corporations	Nuclear, Environment, Cyber	5	Globalisation is a well known long term driver for changes, **similar to 37**
45	Inclusive Security?: United Nations Security Council Enlargement?	Nuclear, Environment, Cyber	1	Global administrative unites changes
46	Public Service, Private Provider?: Future Implications of the Growth of PFI Schemes	Nuclear, Environment, Cyber	1	New processes and innovation in organizational structures
47	Serious, Organized and Networked Crime: Criminal Networks in the era of Globalisation	Nuclear, Environment, Cyber	9	Structural change in police and army operations (Globalisation), **similar to 32**
48	Raising the Stakes: Will Iran Develop Nuclear Capability?	Nuclear	3	Well known threat
49	A Modern Icarus: Could Solar Flares Cause Communication Meltdown?	Nuclear, Environment, Cyber	6	Well known threat, but low probability and high impact
50	Who's Looking at you? Increasing Mass Surveillance	Nuclear, Environment, Cyber	7	Long term trend, but with a potential to become a game changer, occasionally
51	Plenty More Fish in the Sea?: The Depletion of Fish Stocks.	Environment	5	Long term trend, with well known actions to change the trend

52	Sowing a Bitter Crop: Global Reductions in Available Arable Land	Environment	6	Long term trend, with well known actions to change the trend
53	To Arms: The Growing use of Lethal Force in Violent Crime Across Europe	Nuclear, Environment, Cyber	5	Long term trend
54	Talking Rubbish: The Struggle to Conquer the Growing Waste Mountain	Nuclear, Environment	8	Long term trend. In case of nuclear increasing probability for unintended contamination.
55	The Kraken Awakes: the Impact of a Cataclysmic Seismic Event	Environment	10	Low probability high impact disruptive event
56	End-game?: A Major Asteroid Impact on Earth	Environment	10	Low probability high impact disruptive event
57	Gene Out of the Bottle: Could Genes from GMOs Proliferate in Nature?	Environment	10	The GMO might have a high impact in the evolutionary balance.
58	Virtually Criminal: the Rise of Internet Crime	Cyber	8	Long term trend, but with a high potential for disruptive events.
59	The Oil Crisis: Any Light at the End of the Pipeline?	Environment	9	End of oil will be a game changer.
60	Geoshifts in Innovation	Nuclear, Environment, Cyber	9	Could be a game changer for specific regions.
61	Sensors and Tracking: Finding Anything, Anywhere, Anytime	Cyber	8	Long term trend, but with a high potential for disruptive events.
62	Security: Marrying Technological and Human Approaches	Cyber	3	Long term trend.
63	Who's in Charge: Choosing, Funding and Communicating Science Projects	Nuclear, Environment, Cyber	2	Trend
64	Understanding Complexity: How to Answer the Big Questions	Nuclear, Environment, Cyber	1	Trend
65	A Droid for All Seasons: Robots Become More Versatile	Nuclear, Environment, Cyber	7	Long term trend, but with a potential for disruptive events.
66	Synthetic Chemical Cells – A New Way for the Invention, Discovery, Synthesis and Production of Molecules and Materials	Environment	6	Long term innovation trend, but with a potential for disruptive events.
67	Surviving Peak Oil	Nuclear, Environment, Cyber	10	Game changer event,), **similar to 59**
68	Nuclear NIMBY: Meeting the Challenges of Next-Generation Nuclear Waste Management and Public Acceptability	Nuclear	6	Long term problem, but with a potential for disruptive events.
69	Continued Growth in Energy Consumption	Nuclear, Environment	8	Possible long term trend, with a potential for additional disruptive events.
70	Dangerous Climate Change and Tipping Points	Nuclear, Environment, Cyber	10	Disruptive Event

Table 15: List of weak signals, with their potential for a wild card

6.5 Literature

Most important literature sources for the stocktaking of the key factors and future projections.

6.5.1 Theory of scenarios

Behlau, Lothar/ Kulas, Andrea/ Dönitz, Ewa/ Schirrmeister, Elna (2010): *In welcher Zukunft forschen wir? der Europäische Forschungs- und Innovationsraum 2025*. München: Fraunhofer-Gesellschaft.

Gausemeier, J./ Fink, A.; Schlake, O. (1996): *Szenario Management. Planen und Führen mit Szenarien*. Carl Hanser Verlag, München, Wien.

Geschka, Horst/ Reibnitz, Ute v. (1981): *Die Szenario-Technik als Grundlage von Planungen*. Frankfurt am Main: Battelle-Institut e.V.

Godet, Michel (2000): *The Art of Scenarios and Strategic Planning*: Tools and Pitfalls, Technological Forecasting and Social Change, Vol. 65, S. 3-22.

Götze, Uwe (1993): *Szenario-Technik in der strategischen Unternehmensplanung*, 2., aktualisierte Auflage. Wiesbaden: Deutscher Universitäts-Verlag.

Herzhof, Marc (2005): *Szenario-Technik in der chemischen Industrie: Untersuchung von Software-Tools am Beispiel einer Studie zum Markt für Flammschutzmittel im Jahr 2010 und der praktischen Bedeutung der Szenario-Technik*, 1. Auflage. Berlin: Pro Business.

Kosow, Hannah/ Gaßner, Robert (2008): *Methoden der Zukunfts- und Szenarioanalyse. Überblick, Bewertung und Auswahlkriterien*. WerkstattBericht Nr. 103. IZT: Berlin.

Postma, Theo J. B. M./ Liebl, Franz (2005): *How to improve scenario analysis as a strategic management tool*, Technological Forecasting and Social Change, Vol. 72, S. 161-173.

Schomaker, Paul J. H. (1995): *Scenario Planning: A Tool for Strategic Thinking*, in: Sloan Management Review, S. 25-40.

Seidl, David/ Werle, Felix (2011): *Strategisches Management und die Offenheit der Zukunft in: Zukunftsorientierung in der Betriebswirtschaftslehre*, Tiberius, Victor (Hrsg.), Gabler Verlag, Wiesbaden, S. 287-299.

6.5.2 Context

Allied Command Transformation, *"Multiple Futures Project – Navigating towards 2030"*, 2009.

BEFORE: Benchmarking and Foresight for Regions of Europe, *"ICT Sector in Mid Sweden Images of the future for 2020 and the road there – Foresight Study"*, 2008.

Behlau, Lothar, Andrea Kulas, Ewa Dönitz and Elna Schirrmeister, *"Envisioning future research horizons. Scenarios for the European research landscape 2025"*, Fraunhofer-Gesellschaft, München, 2010.

Boden, Mark, Cristiano Cagnin, Vicente Carabias, Karel Haegeman and Totti Könnölä, *"Facing the future: time for the EU to meet global challenges"*, JRC Scientific and Technical Reports, 2010.

Braun, Anette, *"Global Europe 2030 - 2050 – State of the art of international Forward Looking Activities beyond 2030"*, European Commission, 2010.

Butter, Maurits, Miriam Leis, Christine Balch, Totti Könnölä, Victor van Rij, Petra Schaper-Rinkel, Matthias Weber, Joachim Klerx, Ozcan Saritas, Effie Amanatidou and Jennifer Cassingena-Harper, *"SESTI working paper - Major trends, challenges and emerging issues in Health"*, European Commission, 2010.

Cremonini, Leon, Andrew Rathmell and Caroline Wagner, *"Cyber Trust & Crime Prevention: Foresight Overview"*, Office of Science & Technology, UK, 2003.

Endregard, Monica, Hanne Breivik and Hege Schultz, *"Scenario template, existing CBRN scenarios and historical incidents"*, 2011.

Ernst & Young, *"The evolving IT risk landscape"*, 2011.

European Commision, *"FORESEC - Cooperation in the Context of Complexity: European Security in Light of Evolving Trends, Drivers, and Threats"*, 2009.

European Commission, *"Cooperation in the Context of Complexity: European Security in Light of Evolving Trends, Drivers, and Threats"*.

European Commission, *"ESRIF Final Report - Annex IV"*, 2009.

European Commission, *"Facing the future: global challenges in 2025 And EU policy implications"*.

European Commission, *"Foresight on Information Society Technologies in the European Research Area (FISTERA)"*, 2006.

European Commission, "*The World in 2025 – Contributions from an expert group*", European Research Area, 2009.

European Commission, "*The World in 2025 – Rising Asia and Socio-ecological Transition*", European Research Area, 2009.

European Commission, "Inventory of Forward Looking Studies with a focus beyond 2030".

FEMA, *"Crisis Response and Disaster Resilience 2030"*, The Strategic Foresight Initiative (SFI), 2012.

FOI – Swedish Defence Research Agency, *"Nordic ICT Foresight: External Scenarios for the Sociotechnical Environment Around ICT in the Nordic Region"*, 2006.

Government Office for Science, *"Dimensions of Uncertainty"*.

Hague Centre for Strategic Studies, *"STRONG in the 21st Century Strategic Orientation and Navigation Guidance under Deep Uncertainty"*, 2010.

Homeland Security, *"Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty*", FEMA, 2012.

International Council for Science, *"A Science Plan for Integrated Research on Disaster Risk: Addressing the challenge of natural and human-induced environmental hazards"*, 2008.

International Council for Science, *"A Science Plan for Integrated Research on Disaster Risk - Addressing the challenge of natural and human-induced environmental hazards"*, 2008.

Jackson, Jonathan, Nick Allum and George Gaskell, *"Perceptions of risk in cyberspace"*, 2004.

Leitner, Karl-Heinz, "Innovation Futures: A Foresight Exercise on Emerging Patterns of Innovation. Visions, Scenarios and Implications for Policy and Practice" 2012.

Leitner, Karl-Heinz, Francois Jegou, Philine Warnke, Johannes Mahn, Karl-Heinz Steinmüller, Wolfram, Rhomberg, Sivert von Salvern, Elna Schirrmeister and Vanessa Watkins, *"Innovation Futures: A Foresight Exercise on Emerging Patterns of Innovation. Visions, Scenarios and Implications for Policy and Practice – Final Report*", European Commission, 2012.

National Intelligence Council (NIC), *"Global Governance 2025: at a Critical Juncture"*, Office of the Director of National Intelligence, 2010.

National Intelligence Council (NIC), *"Global Trends2025: A Transformed World"*, Office of the Director of National Intelligence, 2008.

National Intelligence Council, *"Global Trends 2025: A Transformed World"*, 2008.

Oertzen, Jürgen von, Kerstin Cuhls and Simone Kimpeler, *"Wie nutzen wir Informations- und Kommunikationstechnologien im Jahr 2020"*, FAZIT Forschung, Forschungsbericht, Vol. 3, 2006.

Rockefeller Foundation, Global Business Network, *"Scenarios for the Future of Technology and International Development"*, 2010.

SANDERA, *"The Future Impact of Security and Defence Policies on the European Research Area"*, 2010.

SANDERA, *"Scenario Report - The Future Impact of Security and Defence Policies on the European Research Area*", Manchester Institute of Innovation Research, UK, 2010.

Sessa, Carlo, Andrea Ricci, Riccardo Enei and Giovanna Giuffrè, *"Qualitative Scenarios"*, PASHMINA, 2010.

SESTI, *"Major trends, challenges and emerging issues in Health"*, 2010.

Sicherheitsforum Deutsche Wirtschaft e.V., *"Zukunftsstudie Security 2015: Welche Faktoren beeinflussen die Sicherheit deutscher Global Player im Jahr 2015?"*, 2006.

SmartMeme, *"The Future of Foresight Long Term Strategic Considerations for Promoting the Precautionary Principle"*, 2006.

SmartMeme, *"The Future of Foresight - Long Term Strategic Considerations for Promoting the Precautionary Principle"*, 2006.

Spiegeleire, Stephan de, Tim Sweijs, Jaakko Kooroshy, Aurélie and Basha i Novosejt, *"STRONG in the 21th Century – Strategic Orientation and Navigation Guidance under Deep Uncertainty"*, The Hague Centre for Strategic Studies No 04 | 07 | 10, 2010.

Ulied, Andreu, Oriol Biosca and Rafael Rodrigo, *"Forecast and quantitative scenarios, as an evolution of the qualitative"*, PASHMINA, 2010.

UNIDO, *"Foresight Methodologies"*, 2004.

World Economic Forum, *"Global Risks 2012, Seventh Edition"*, 2012.

World Economic Forum, *"The Global Risks 2011, Sixth Edition"*, 2011.

Zukunftsinstitut GmbH, *"Die Netzgesellschaft – Schlüsseltrends des digitalen Wandels"*, 2011.

6.5.3 Cyber infrastructure

Balzarotti, Davide (ed.), *"Deliverable 4.1: First Report on Threats on the Future Internet and Research Roadmap"*, SysSec, European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet, Seventh Framework Programme, Grant Agreement no. 257007, 2011. http://www.syssec-project.eu/media/page-media/3/syssec-d3.2-first-summer-school.pdf

Bizer, Johann, Kai Dingel, Benjamin Fabian, Oliver Günther, Markus Hansen, Michael Klafft, Jan Möller, Sarah Spiekermann, *"Technikfolgenabschätzung - Ubiquitäres Computing und Informationelle Selbstbestimmung"*, Bundesministerium für Bildung und Forschung (BMBF), 2008.

Bundesamt für Sicherheit in der Informationstechnik, *"Register aktueller Cyber-Gefährdungen und -Angriffsformen"*, BSI-Analysen zur Cyber-Sicherheit 001, Version 1.00, 16. January 2012. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf?__blob=publicationFile

Borchgrave, Arnaud de, Frank J. Cilluffo, Sharon L. Cardash, Michèle M. Ledgerwood, *"Cyber Threats and Information Security Meeting the 21st Century Challenge"*, Center for Strategic and International Studies, Washington, D.C., 2000.

Botterman, Maarten, Jonathan Cave, James P. Kahan, Neil Robinson, Rebecca Shoob, Robert Thomson and Lorenzo Valeri, *"Cyber Trust and Crime Prevention:Gaining Insight from Three Different Futures"*, Office of Science and Technology, United Kingdom, 2004.

Carlsen, Henrik, *"Nordic ICT Foresight. External Scenarios for the Socio-technical Environment Around ICT in the Nordic Region"*, Nordic Innovation Centre, Project number: 04263, May 2006. http://nordic-ictfore.vtt.fi/materiaali/carlsen_nordic%20ict%20foresight%20scenario%20report.pdf

Siemens AG (ed.), "People to watch: Raymond Kurzweil. Ein Traum von einem Mann", *Industry Journal,* No. 02, 2011, pp. 62-65. http://www.siemens.com/industryjournal/pool/02-2011/01_78_Komplett_301_D.pdf

Catteddu, Daniele, *"Security & Resilience in Governmental Clouds"*, European Network and Information Security Agency (ENISA), 2011.

Cisco, *"The Evolving Internet Driving Forces, Uncertainties, and Four Scenarios To 2025"*, Cisco and Global Business Network (GBN), 2010.

Coleman, Nick, *"Smart Cloud"*, IBM Corporation, 2012.

Coleman, Nick and Martin Borrett, *"Cloud Security. Who do you trust?"*, IBM Corporation, 2010.

Dekker, Marnix and Christofer Karsberg, *"Annual Incident Reports 2011 - Analysis of the Article 13a incident reports of 2011"*, European Network and Information Security Agency (ENISA), 2012.

Diehn, Timur, "Constanze Kurz: Die Datenprofiteure", *Stifterverband-Magazin "Wirtschaft & Wissenschaft"*, No. 1, 2012, pp. 40-43. http://www.stifterverband.info/meinung_und_debatte/2012/kurz_datenprofiteure_digitale_muendigkeit/wuw_2012-01_constanze_kurz.pdf

Döbler, Thomas, *"Potenziale von Social Software"*, FAZIT Forschung, Forschungsbericht, Vol. 5, December 2007.

Egozcue, Elyoenai, Daniel Herreras Rodríguez, Jairo Alonso Ortiz, Victor Fidalgo Villar and Luis Tarrafeta, *"Smart Grid Security - Recommendations for Europe and Member States",* European Network and Information Security Agency (ENISA), 2012.

Federal Office for Information Security, *"The IT Security Situation in Germany 2011",* Bonn, 2011. http://secunia.com/?action=fetch&filename=it-security-situation-in-germany-2011.pdf

Fichtner, Johan, *"Siemens Reaction to Cybersecurity Challenges",* Cybersecurity 2011, Berlin, 14.09.2011.

Foley, Brian, "*Think Tank for Converging Technical and Non-Technical Consumer Needs in ICT Trust, Security and Dependability*", Think Trust, 2010.

Frickel, Claudia, "*Viren-Experte: 'Wir sind für den Cyber-Krieg nicht gerüstet'. Kasperskys apokalyptische Vision auf der DLD*", Focus online, 21.01.2013. http://www.focus.de/digital/internet/tid-29140/kasperskys-apokalyptische-vision-auf-der-dld-viren-experte-wir-sind-fuer-den-cyber-krieg-nicht-geruestet_aid_900988.html

Gaycken, Sandro and Dr. Michael Karger, "*Entnetzung statt Vernetzung - Paradigmenwechsel bei der IT-Sicherheit*", MultiMedia und Recht (MMR), Vol. 1, 2011.

Haderlein, Andreas and Janine Seitz, "*Die Netzgesellschaft. Schlüsseltrends des digitalen Wandels*", Zukunftsinstitut GmbH, Kelkheim, 2011.

Hallinan, Dara; Michael Friedewald and Paul McCarthy, "Citizens' perceptions of data protection and privacy in Europe", Computer Law & Security Review, Vol. 28, Issue 3, June 2012, pp. 263-272. http://www.sciencedirect.com/science/article/pii/S026736491200057X

Hange, Michael, "*Schutz und Sicherheit kritischer Informations und Kommunikations-Infrastrukturen*", Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2010.

Hartmann, Bernd, Andrea Buchholz and Bernd Beckert (eds.), "*Sicherheit durch IT. Marktchancen und Herausforderungen am Beispiel Baden-Württemberg",* FAZIT Forschung, Forschungsbericht, Vol. 14, July 2008.

Homeland Security, "*Blueprint for a Secure Cyber Future, The Cybersecurity Strategy for the Homeland Security Enterprise*", Homeland Security, 2011.

Kraftschik, Florian, "*Mensch-Maschinen, Wirklichkeitsmaschinen. Eine exemplarische Studie zur Rolle der Science Fiction in der Zukunftsforschung",* Magisterarbeit, Albert-Ludwigs-Universität Freiburg i. Br., 2012. http://www.medialphysisch.de/wp-content/uploads/2013/03/Kraftschik_Mensch-Maschinen_Wirklichkeitsmaschinen_FullA.pdf

Krüger, Kristin, "IT-Sicherheit in der öffentlichen Wahrnehmung", *Magdeburger Journal zur Sicherheitsforschung*, Vol. 1, 2012, pp. 153-167.

Lord, Kristin M. and Travis Sharp, "America's Cyber Future *Security and Prosperity in the Information Age*", Vol. II, Center for a New American Security, 2011.

Lotz, Volkmar, "Towards a Secure and Trusted Business Web", in Neeraj Suri and Michael Waidner (eds.), *"Sicherheit 2012: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 7.-9. März 2012 in Darmstadt",* Darmstadt, 2012, pp. 4-5.

Marcus, Alan, "*Risk and Responsibility in a Hyperconnected WorldPathways to Global Cyber Resilience*", World Economic Forum, 2012.

Minkwitz, Oliver, "*Ohne Hemmungen in den Krieg? – Cyberwar und die Folgen*", HSFK-Report 10/2003, Hessische Stiftung Friedens- und Konfliktforschung, 2003.

Nelson, Michael R., "*Cloud Computing and Public Policy, Briefing Paper for the ICCP Technology Foresight Forum*", OECD Publishing, DSTI/ICCP(2009)17, 2009.

Ottenberg, Carsten, Susanne Kunschert and Prof. Dr. August-Wilhelm Scheer, "*Promotorenbericht zum Zukunftsprojekt Sichere Identitäten*", Promotorengruppe Sicherheit der Forschungsunion Wirtschaft-Wissenschaft, 2012.

Ozler, Yunus and Pippa Thomas, "The digitization of everything", *Performance,* Think Tank for Business Performance & Innovation, Vol. 4, Issue 3, June 2012, pp. 26-37. http://performance.ey.com/wp-content/plugins/download-monitor/download.php?id=229

Pitkänen, Olli, Risto Sarvas, Asko Lehmuskallio, Miska Simanainen, Vesa Kantola, Mika Rautila, Arto Juhola, Heikki Pentikäinen and Ossi Kuittinen, "*Future Information Security Trends*, Final Report", Helsinki Institute for

Information Technology (HIIT), 2011.

President's Information Technology Advisory Committee, "*Cyber Security: A Crisis of Prioritization*", published by the National Coordination Office for Information Technology Research and Development, 2005.

Robinson, Neil, Emma Disley, Dimitris Potoglou, Anais Reding, Deidre Culley, Maryse Penny, Maarten Botterman, Gwendolyn Carpenter, Colin Blackman and Jeremy Millard, *"Feasibility study for a European Cybercrime Centre. Final report"*, RAND Europe, 2012.

Sando, Sven and Patrick Fink, "Off limit: controlling employee information access", *Performance,* Think Tank for Business Performance & Innovation, Vol. 4, Issue 4, November 2012, pp. 46-51. http://performance.ey.com/wp-content/plugins/download-monitor/download.php?id=356

Schaffry, Andreas, "Incident Report - Die Gründe für Internetausfälle", Computerwoche, http://www.computerwoche.de/a/die-gruende-fuer-internetausfaelle,2526966, 2012.

Seidler, Felix F., "*Sicherheitsumfeld Cyber-Space: Abhängigkeiten, Akteure, Herausforderungen und Perspektiven*", Magdeburger Journal zur Sicherheitsforschung, Vol. 2, 2011, pp. 102-114.

Sommer, Peter and Ian Brown, *"Reducing Systemic Cybersecurity Risk - OECD/IFP Project on 'Future Global Shocks'"*, OECD Publishing, 2011.

Stall, Sascha Tessier, "*The Future Of Cybersecurity*", PAPER No. 2011•04, The Hague Centre for Strategic Studies and TNO, 2011.

SysSec, European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet, *"System Security Research in Europe: A Research Roadmap"*, Seventh Framework Programme, Grant Agreement no. 257007, 2012. http://www.syssec-project.eu/media/page-media/3/system-security-research-roadmap-whitepaper.pdf

Forward, Managing Emerging Threats in ICT infrastructure, *"Deliverable D3.1: White book: Emerging ICT Threats"*, Seventh Framework Programme, Grant Agreement no. 216331, 2010. http://www.ict-forward.eu/media/publications/forward-whitebook.pdf

Teller, Tomer, *"The Biggest Cybersecurity Threats of 2013"*, Forbes, 12. May 2012. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf?__blob=publicationFile

TNS Opinion & Social, "*Cyber security - Special Eurobarometer 390*", European Commission, 2012.

Uddenfeldt, Jan, Peder Ramel, Lars Stugemo, Östen Mäkitalo, Staffan Truvé and Marianne Treschow, "*AMBIENT SWEDEN Internet Foresight – How Sweden will become a leading Internet nation in 2015*", The Royal Academy of Engineering Sciences (IVA), 2008.

Verhees, Pieter, Astrid Wisse and Bart Reede, "How will consumers communicate, in 2020?", *Performance,* Vol. 4, Issue 4, November 2012, pp. 32-39. http://performance.ey.com/wp-content/plugins/download-monitor/download.php?id=354

Working group experts of European Network and Information Security Agency (ENISA), "*Economics of Security*: *Facing the Challenges - A multidisciplinary assessment*", European Network and Information Security Agency (ENISA), 2012.

Wüest, Candid, *"Symantec Security-Trends 2012. Was war 2011 und worauf müssen wir uns einstellen?",* Symantec, 2012. http://m.pressebox.de/attachment/431794/1.pdf

6.5.4   Nuclear

Alger, Justin, "A Guide to Global Nuclear Governance: Safety, Security and Nonproliferation", Centre for International Governance Innovation, 2008.

Alvarez, Robert, "Radioactive Waste and the Global Nuclear Energy Partnership", Institute for Policy Studies, 2007.

ANSTO, "Management of Radioactive Waste in Australia", 2011. http://www.ansto.gov.au/__data/assets/pdf_file/0020/46172/Management_of_Radioactive_Waste_in_Australia_v2.pdf

Appel, Detlef and Jürgen Kreusch, "Sicherheitstechnische und gesellschaftliche Aspekte von Monitoring bei der Endlagerung radioaktiver Abfälle mit Option ihrer Rückholbarkeit", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 52-58.

Apostolakis, George, Pavel Hejzlar and Eugene Shwageraus, "The Future Of The Nuclear Fuel Cycle", Massachusetts Institute of Technology, 2010.

Baisden, Patricia and Gregory Choppin, "Nuclear Waste Management and the Nuclear Fuel Cycle", Encyclopedia of Life Support Systems, 2007.

Bayne, Emmalee, "Radioactive Waste Management", White Word Publications, 2012.

Beránek, Jan, Rianne Teule and Aslihan Tumer, "The deadly legacy of radioactive waste – Wasting our time with nuclear power", Greenpeace International, 2010.

Beuth, Thomas, Bruno Baltes, Wilhelm Bollingerfehr, Dieter Buhmann, Frank Charlier, Wolfgang Filbert, Klaus Fischer-Appelt, Jörg Möning, Andre Rübel and Jens Wolf, "Untersuchungen zum menschlichen Eindringen in ein Endlager. Vorläufige Sicherheitsanalyse für den Standort Gorleben", Gesellschaft für Anlagen- und Reaktorensicherheit (GRS) mbh, No. 280, Köln, 2012.

Bergmans, Anne, Mark Elam, Peter Simmons and Göran Sundqvist, "Perspectives on Radioactive Waste Repository Monitoring", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 22-27.

BESAFE Project, "Partners", 2012. http://besafe-project.net/page.php?P=26&SP=3

Botella, T., J. Coadou and U. Blohm-Hieber, "European citizens' opinions towards radioactive waste: an updated review", European Comission, Directorate General for Energy and Transport Unit Nuclear Energy and Radioactive Waste, 2005.

Brasser, Thomas, Johannes Droste, Ingo Müller-Lyda, Julia Mareike Neles, Michael Sailer, Gerhard Schmidt and Mathias Steinhoff, "Endlagerung wärmeentwickelnder radioaktiver Abfälle in Deutschland", Gesellschaft für Anlagen- und Reaktorensicherheit (GRS) mbh, No. 247, 2008.

Brunnengräber, Achim, Lutz Metz, Maria Rosaria Di Nucci and Miranda Schreurs, "Nukleare Entsorgung: Ein 'wicked' und höchst konfliktbehaftetes Gesellschaftsproblem", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012, pp. 59-65.

Bundesministerium für Bildung und Forschung, "Verbund bündelt Kompetenzen der Entsorgungsforschung", Pressemitteilung Nr. 149/2012, 3. December 2012.

Burns, W., A. Hughes, J. Marples, R. Nelson and A. Stoneham, "Effects of Radiation on the Leach Rates of Vitrified Radioactive Waste", Journal of Nuclear Materials, 1982.

Cantlon, John E.; "Nuclear Waste Management in the United States The Nuclear Waste Technical Review Board's Perspective", Topseal Conference, 1996.

Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage, "Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report", National Academy of Sciences, 2006. http://www.nap.edu/catalog/11263.html

Compañó, Ramón, Corina Pascu, Jean-Claude Burgelman, Michael Rader, Roberto Saracco, Graziella Spinelli, Bernhard Dachs, Matthias Weber, Sami Mahroum, Rafael Popper, Lawrence Green and Ian Miles, "Foresight on Information Society Technologies in the European Research Area (FISTERA) - Key Findings", European Commission, 2006.

Council of the European Union, "Community framework for the responsible and safe management of spent fuel and radioactive waste", Council Directive 2011/70/EURATOM of 19.07.2011.

Department for Environment, Food and Rural Affairs, Department of the Environment, National Assembly of Wales, Scottish Executive, "Managing Radioactive Waste Safely", 2001. http://www.sepa.org.uk/radioactive_substances/publications/idoc.ashx?docid=3cf671f4-4e74-4307-8eab-3cbb6a08e52b&version=-1

derStandard.at GmbH, "Atomkraftwerke in Europa", 2010. http://derstandard.at

Deutch, John M., Dr. Charles W. Forsberg, Prof. Andrew C. Kadak, Prof. Mujid S. Kazimi, Prof. Ernest J. Moniz and Dr. John E. Parsons, "Update of the MIT 2003 Future Of Nuclear Power", Massachusetts Institute of Technology, 2009.

Di Pace, Luigi, Laila El-Guebaly, Boris Kolbasov, Vincent Massaut and Massimo Zucchetti, "Radioactive Waste

Management of Fusion Power Plants", Croatia, 2012.

Dieckhoff, C., W. Fichtner, A. Grunwald, S. Meyer, M. Nast, L. Nierling, O. Renn, A. Voß and M. Wietschel, "Energieszenarien – Konstruktion, Bewertung und Wirkung – ‚Anbieter' und ‚Nachfrager' im Dialog", KIT Scientific Publishing, 2011.

Ebinger, Charles and Kevin Massy, "Security Implications of the Expansion of Nuclear Energy", The Brookings Institution, 2009.

Energy & Biodiversity Initiative, "Participating Organizations". www.theebi.org/pdfs/organizations.pdf

Environment Literacy Council, National Science Teachers Association, "Radioactive Waste: Resources for Environmental Literacy", National Science Teachers Association Press, 2007.

European Commission, "Europeans and Nuclear Safety. Report", Special Eurobarometer 271, 2007. http://www.ec.europa.eu/public_opinion/archives/ebs/ebs_271_en.pdf

European Commission, "Global Europe 2050. Executive Summary", 2011. http://ec.europa.eu/research/social-sciences/pdf/global-europe-2050-summary-report_en.pdf

European Commission, "Roadmap. Nuclear Safety", 2011. http://ec.europa.eu/governance/impact/planned_ia/docs/2012_ener_010_nuclear_safety_en.pdf

European Nuclear Society, "Nuclear Power Plants in Europe", 2013. http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-europe.htm

Ewing, R., B. Chakoumakos, G. Lumpkin, T. Murakami, R. Greegor, F. Lytle, "Metamict Minerals: Natural Analogues for Radiation Damage Effects in Ceramic Nuclear Waste Forms", Nuclear Instruments and Methods in Physics Research, 1988.

Ewing, R., W. Weber and F. Clinard, Jr., "Radiation Effects in Nuclear Waste Forms for High-Level Radioactive Waste", Pergamon, 1994.

Fitzpatrick, Mark and Tim Huxley, "Preventing Nuclear Dangers in Southeast Asia and Australasia, Chapter 3: Nuclear Safety and Security", International Institute for Strategic Studies, Washington, DC, 2009.

Forschungszentrum Jülich, „Impact of Partitioning, Transmutation and Waste Reduction Technologies on the Final Nuclear Waste Disposal", Energy and Environment, Vol. 15, 2007.

Frinking, Erik, Tim Sweijs, Teun van Dongen and Aksel Ethembabaoglu, "Navigating thecbrn landscape of 2010 and beyond: towards a new policy paradigm", The Hague Center for Strategic Studies, No 01 | 01 | 10, 2009.

Greenwald, Janet, "Whoops! Nuke Waste Wreck Would Rack Local Economy", Synthesis/Regeneration 11, Fall 1996. http://www.greens.org/s-r/11/11-06.html

Griessler, Erich and Peter Biegelbauer, "What a Difference a p(TA) Makes", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 73-75.

Grunwald, Armin, "Editorial", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., p. 4.

Haney, Johannah, "Nuclear Energy", Benchmark, 2012.

Harness, Sharon, "Anti-Nuclear Movements (World Study)", University Publications, 2012.

Health and Safety Executive, "Management of Radioactive Material and Radioactive Waste on Nuclear Licensed Sites", Nuclear Safety Directorate, 2001.

Hench, L., D. Clark and J. Campbell, "High Level Waste Immobilization Forms", Pergamon Press Ltd., 1984.

Herlugson, Chris, "bp experience in biodiversity conservation", Fifth World Parks Congress, Durban, South Africa, 2003.

Hocke, Peter, Anne Bergmans and Sophie Kuppler, "Guaranteeing Transparency in Nuclear Waste Management: Monitoring as Social Innovation", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012, pp. 10-14.

Holt, Mark and Anthony Andrews, "Nuclear Power Plant Security and Vulnerabilities", Congressional Research Service, 2012.

Holt, Mark, "Civilian Nuclear Waste Disposal", Congressional Research Service, 2011.

International Atomic Energy Agency, „Determination and use of scaling factors for waste characterization in nuclear power plants", IAEA nuclear energy series, no. NW-T-1.18, Vienna, 2009.

International Atomic Energy Agency, "Developing multinational radioactive waste repositories: Infrastructural framework and scenarios of cooperation", Austria, 2004.

International Atomic Energy Agency, "Directory of National Regulatory Bodies for the Control of Radiation Sources", http://www-ns.iaea.org/downloads/rw/code-conduct/reg-auth-directory.pdf, 2012.

International Atomic Energy Agency, "Disposal of Radioactive Waste Specific Safety Requirements", http://www-pub.iaea.org/MTCD/publications/PDF/Pub1449_web.pdf, 2007.

International Atomic Energy Agency, "Environmental and Ethical Aspects, Radioactive Waste Management – Appendix 5", 2012. http://www.world-nuclear.org/info/Environmental_Ethical_Aspects_inf04ap5.html

International Atomic Energy Agency, "Fundamental Safety Principles. Safety Fundamentals", IAEA Safety Standards Series No. SF-1, Vienna, 2006.

International Atomic Energy Agency, "Geological disposal of radioactive waste. Technological implications for retrievability", IAEA nuclear energy series, no. NW-T-1.19, Vienna, 2009.

International Atomic Energy Agency, "Handbook on photonuclear data for applications. Cross-sections and spectra", Vienna, 2000.

International Atomic Energy Agency, "Long Term Structure of the IAEA Safety Standards and Current Status", 2012. http://www-ns.iaea.org/committees/files/CSS/205/status.pdf

International Atomic Energy Agency, „Viability of sharing facilities for the disposal of spent fuel and nuclear waste. An assessment of recent proposals", Vienna, 2011.

INFORUM Verlags- und Verwaltungsgesellschaft, "Länder mit Kernkraftwerken in Betrieb", www.kernenergie.de, 2012.

International Energy Agency, "World Energy Outlook 2011", IEA Publications, 2011.

Kallenbach-Herbert, Beate and Stefan Alt, "Monitoring als Baustein für die Entscheidungsfindung in Endlagerprojekten", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012, pp. 15-21.

Kallenbach-Herbert, Beate and Dr. Bettina Brohmann,, "D1.1. Descriptive overview of governance models", OBRA, 2007.

Kallenbach-Herbert, Beate and Dr. Bettina Brohmann, "Models of Governance and Success Factors", Co-ordination Action, European Observatory for Long-term Governance on Radioactive Waste Management OBRA (2006-2008), First Workshop, Eurajoki, Finland, 1. February 2007.

Koelzer, Winfried, "Glossary of Nuclear Terms", Forschungszentrum Karlsruhe GmbH, 2012.

Kringiel, Danny, "Nuklearkatastrophe in Brasilien. Verführt vom Schimmer des Todes", Spiegel Online, 2012. http://einestages.spiegel.de/s/tb/25584/goiania-unfall-1987-nuklearkatastrophe-in-brasilien.html

Landström, Catharina and Jan-Willem Barbier, "The Challenge of Long-term Participatory Repository Governance", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 66-72.

Lidskog, Rolf and Ann-Cathrin Andersson,"The management of radioactive waste A description of ten countries", Svensk Kärnbränslehantering AB. http://www.edram.info/fileadmin/edram/pdf/The_management.pdf

Lammer, M. and A. L. Nichols, „Fission product yield data for the transmutation of minor actinide nuclear waste", International Atomic Energy Agency, Vienna, 2008.

Leite, Marco Antônio Sperb and L. David Roper, "The Goiâna Radiation Incident. A Failure of Science and Society", 1988. http://arts.bev.net/roperldavid/gri.htm

Lillington, John N., "The Future of Nuclear Power", Elsevier Science, 2004.

Matthes, Felix Chr. and Hauke Herrmann, "Contribution to the consultation on generation adequacy, capacity mechanisms and the internal market in electricity", Institute for Applied Ecology, Berlin, 2013.

Matzke, Hj.,"Radiation Damage Effects in Nuclear Materials", Nuclear Instruments and Methods in Physics Research, 1988.

Moussaid, M. and G. Degreef, "Country Report for Belgium", Belgian Nuclear Society – Young Generation Network, Brussels, 2011.

Murray, James, Joseph Harrington and Richard Wilson, "Chemical and Nuclear Waste Disposal: Problems and Solutions", Cato Journal, 1982.

Narayan, P.K., "Chapter 17 – Disposal of Radioactive Waste", Barch Higlights. http://www.barc.gov.in/publications/eb/golden/nfc/toc/Chapter%2017/17.pdf

NATO, "Multiple Futures Project – Navigating towards 2030", 2009.

Nentwich, Michal and Ulrich Riehm, "Internationale Fachportale für Technikfolgenabschätzung", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 76-95.

Neumann, Wolfgang, "Nuclear Waste Management in the European Union: Growing Volumes and No Solution", INTAC, Hanover, 2010.

Nuclear Decommissioning Authority, "The 2010 United Kingdom Radioactive Waste & Materials Inventory", Contractors Report to NDA, 2011.

Nuclear Energy Institute, "Nuclear Waste Disposal for the Future: The Potential of Reprocessing and Recycling", 2006. http://www.nei.org/resourcesandstats/Documentlibrary/Nuclear-Waste-Disposal/whitepaper/reprocessingandrecycling

Nuclear Threat Initiative, "NTI Nuclear Materials Security Index – Building a Framework for Assurance, Accountability and Action", The Economist, 2012.

Nuclear Threat Initiative, "Understanding Nuclear Threats", 2013. http://www.nti.org/threats/nuclear/

Nuttall, William, "Nuclear Waste Management", Science and Public Affairs, 2003.

OECD, "Methods for Safety Assessment of Geological Disposal Facilities for Radioactive Waste", Nuclear Energy Agency, 2012.

OECD, "Scenario Development Methods and Practice", Nuclear Energy Agency, 1999.

Paes Cunha, Renato de, "Speech", The World Uranium Hearing, Salzburg, 1992. http://www.ratical.org/radiation/WorldUraniumHearing/RenatoDePaesCunha.txt.

Pistner, Christoph, "Nuclear Regulatory Systems", Global Conference for a Nuclear Power Free World 2, Tokyo, 15.-16. December 2012.

Price Stephane "Sectoral trends in global energy use and greenhouse gas emissions", Lawrence Berkeley National Laboratory, Environmental Energy, Technologies Division, Elsevier, 2008.

Raj, K., N.K. Bansal and K.K. Prasad, "Radioactive waste management practices in India", Mumbai, India, 2006.

Risoluti, Piero, "Radioactive waste repositories", Italy, 2011.

Royal Society of Chemistry, "Materials for Nuclear Waste Management", London, 2006.

Sailer, Michael, "Nuclear Energy, Renewable Energy and Peace", Asian Regional Conference "Renewable Energy and Peace", Seoul, Korea, 19.-20. August 2004.

Spiegel, "Tödlicher Stein", No. 42, 1987, p. 173.

Taylor, Derek M., "The future of radioactive waste management", European Commission.

Union of Concerned Scientists, "Reprocessing and Nuclear Waste", Cambridge, 2009.

Vernaz, Etienne Y., "Nuclear waste in France: Current and future practice", London, 2006.

Whitfield, Stephen C., Eugene A. Rosa, Amy Dan and Thomas Dietz, "The Future of Nuclear Power: Value Orientations and Risk Perception", Risk Analysis, Vol. 29, No. 3, 2009, pp. 425-437.

Wikipedia, "Radioactive waste", http://en.wikipedia.org/wiki/Radioactive_waste, 2013.

Wikipedia, "Waste management in Bangladesh", 2013.

 http://en.wikipedia.org/wiki/Waste_management_in_Bangladesh

Wilkinson, Peter, "The future for nuclear: radioactive waste management", 2007.

Wimmer, Hannes, Klaus-Jürgen Brammer and Michael Köbl, "Monitoring im Endlager: notwendig für die Akzeptanz", Technikfolgenabschätzung – Theorie und Praxis, Vol. 21, No. 3, December 2012., pp. 28-32.

World Nuclear Association, "Waste Management", December 2012. http://www.world-nuclear.org/education/wast.htm

Yoshihiko Sumi and Yuichiro Matsuo, "Nuclear Fuel Recycling and Waste Management in Japan", Texas, 2005.

6.5.5   Environment

Alberini, Anna, Ian Bateman, Graham Loomes and Milan Ščasný, "Valuation of Environment-Related Health Risks for Children", OECD Publishing, 2010.

Alcamo, Joseph, Neville J. Ash, Colin D. Butler et al., "Ecosystems and Human Well-being. A Framework for Assessment", Island Press, Washington, DC, 2003.

Aguiar, Martin R., "Biodiversity in Grasslands. Current Changes and Future Scenarios", Food and Agriculture Organization of the United Nations.

Alexander L; Aurora H; Ernesto V, Bepsy C., "Livelihoods and Biodiversity Futures: Building Scenarios for the Térraba River Basin, the Greater Kruger Park, the Warana River Basin, Ba Be National Park and Na Hang Nature Reserve", 2010. http://www.livediverse.eu

Alkemade, Rob, "A Framework to Investigate Options for Reducing Global Terrestrial Biodiversity Loss", Bilthoven, 2009.

Beck, M.B., "Environmental foresight and structural change", Warnell School of Forest Resources, University of Georgia, Athens, GA 30602-2152, USA, 2004. http://www.elsevier.com/locate/envsoft

Bengston, David N., Georg H. Kubik and Peter C. Bishop, "Strengthening environmental foresight: potential contributions of futures research. " Ecology and Society, Vol. 17, No. 2, Article 10, 2012. http://dx.doi.org/10.5751/ES-04794-170210

Bovarnick, A., F. Alpizar, C. Schnell, et al., "The Importance of Biodiversity and Ecosystems in Economic Growth and Equity in Latin America and the Caribbean: An economic valuation of ecosystems", United Nations Development Programme, 2010.

Braun, Anette, "Forward Looking Studies. State-of-the-Art. Paper prepared in view of the first meeting of the Expert Group on Global Europe 2030-2050", Düsseldorf, 2010.

Brunekreef, Bert and Stephen T Holgate, "Air pollution and health", THE LANCET, Vol. 360, 19th October 2002, pp. 1233-1242.

Brzoska, Michael, Dr. Walter E. Feichtinger, Prof. Dr. Hans J. Giessmann, Prof. Dr. Heiner Hänggl, Heinz-Dieter Jopp and Dr. Patricia Schneider, "Klimawandel und Sicherheit", Sicherheit und Frieden, Nomos, 2009.

Bundesministerium für Bildung und Forschung, "Forschung für die zivile Sicherheit 2012 – 2017. Rahmenprogramm der Bundesregierung", Bonn, Berlin, 2012. http://www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf

Carpenter, Stephen R. et al, "The Future of Synthesis in Ecology and Environmental Sciences", based on a workshop held 9.-10. December 2008 in Arlington, Virginia.

Centre for Environmental Research, "Towards integrated long-term scenarios for assessing biodiversity risks", Cologne, Germany, 2006.

Center for European Security Studies (CEUSS), "Results of the FOCUS comprehensive scenario assessment questionnaire", Sigmund Freud University Vienna, 2012. http://www.focusproject.eu/documents/14976/66a8b356-26e5-420b-bf3d-ff47e404acc4

Cludius, Johanna, Hannah Förster and Verena Graichen, "GHG Mitigation in the EU: An Overview of the Current Policy Landscape", World Resources Institute, Washington, DC, 2012. http://pdf.wri.org/ghg_mitigation_eu_policy_landscape.pdf

Dosch, Fabian, "Siedlungsflächenentwicklung und Nutzungskonkurrenzen", Technikfolgenabschätzung – Theorie und Praxis, Vol. 17, No. 2, September 2008, pp. 41-51.

Druel, E., Billé, R. and Treyer, S., "A legal scenario analysis for marine protected areas in areas beyond national jurisdiction", report from the boulogne-sur-Mer seminar, 2011.

European Commission, "Citizens' summary. Agriculture in Europe after 2013". http://ec.europa.eu/agriculture/cap-post-2013/communication/citizens-summary_en.pdf

European Commission, "Global Europe 2050", Directorate-General for Research and Innovation, EUR 25252, Luxembourg, 2012.

European movement for Food Sovereignty and another Common Agricultural Policy (FoodSovCap), "Commentary on the CAP post 2013 legislative proposals", 2013. http://www.nyelenieurope.net/foodsovcap/19-commentary-on-the-cap-post-2013-legislative-proposals

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU), "Biodiversity of surface waters, floodplains and groundwater", Bonn, 2008.

Finkenrath, Matthias, Julian Smith and Dennis Volk, "Analysis of the Globally Installed Coal-Fired Power Plant Fleet", International Energy Agency (IEA), 2012.

Food and Agriculture Organization of the United Nations, "Biodiversity for Food and Agriculture Contributing to food security and sustainability in a changing world", Rome, 2010.

Freibauer, Annette, Erik Mathijs, Gianluca Brunori, Zoya Damianova, Elie Faroult, Joan Girona i Gomis, Lance O´Brien and Sébastien Treyer, "Sustainable food consumption and production in a resource-constrained world", European Commission – Standing Committee on Agricultural Research (SCAR), The 3rd SCAR Foresight Exercise, 2012. http://ec.europa.eu/research/agriculture/scar/pdf/scar_feg_ultimate_version.pdf

GEO Architecture Implementation Pilot, "eHabitat - Climate Change and Biodiversity WG Use Scenario Engineering Report", 2011.

Godfray, Charles, Professor Ian Crute, "Foresight The Future of Food and Farming Challenges and choices for global sustainability", Final Project Report, The Government Office for Science, London, 2011.

Guo, L. B. and Gifford, R. M., "Soil carbon stocks and land use change: a meta analysis", Global Change Biology 8, 2002, pp. 345-360.

Gupta, Harsh, Dr Daniel Murdiyarso, "Science Plan on Hazards and Disasters, Special Vulnerability of Island", International Council for Science (ICSU), 2008.

Hejazi, Mohamad, James Edmonds, Leon Clarke, Page Kyle, Evan Davies, Vaibhav Chaturvedi, Marshall Wise, Pralit Patel, Jiyong Eom, Katherine Calvin, Richard Moss and Son Kim, "Long-term global water projections using six socioeconomic scenarios in an integrated assessment modeling framework", Technological Forecasting & Social Change, 2013. http://dx.doi.org/10.1016/j.techfore.2013.05.006

Herold, M., Couclelis, H. and Clarke, K. C., "The role of spatial metrics in the analysis and modeling of urban land use change", Department of Geography, University of California Santa Barbara, 2003.

Hinners, S. J., Kearns, C. A. and Wesman, C. A., "Roles of scale, matrix, and native habitat in supporting a diverse suburban pollinator assemblage", Ecological Applications, Vol. 22, No. 7, 2012, pp. 1923-1935.

Holsinger, Kent E., "Global Biodiversity Patterns", Stanford, 2003.

Hulme, Philip E., David Roy, Teresa Cunha and Tor-Björn Larsson, "A pan-European inventory of alien species: rationale, implementation and implications for managing biological invasions", in DAISIE (eds.), The Handbook of European Alien Species, Springer, Dordrecht, 2008, pp. 1-18.

iKNOW project, "Wild cards", European Commission, European Research Area, Seventh Framework Programme. www.iknowfutures.eu

Institute for European Environmental Policy (IEEP), "Scenarios and models for exploring future trends of biodiversity and ecosystem services changes", final report to the European Commission, DG Environment on Contract ENV.G.1/ETU/2008/0090r, 2009.

Institute for European Environmental Policy, "Institute for European Environmental Policy", London, 2009.

Intergovernmental Panel on Climate Change (IPCC), "IPCC Special Report Emissions Scenarios", 2000.

Intergovernmental Panel on Climate Change, "Climate Change and Biodiversity", 2002.

International Energy Agency (IEA), "Renewable Energy Medium-Term Market Research, Market Trends and Projections to 2017", OECD Publishing and IEA, 2012.

King, David, "Foresight Future Flooding, Chapter 7 Environmental impacts of future flood risk", Foresight Directorate DTI, 1, London. http://www.foresight.gov.uk

Lambin, Eric F., et al., "The causes of land-use and land-cover change: moving beyond the myths", Global Environment Change, Vol. 11, 2001, pp. 261-269.

Leadley, Paul, "CBD – Global Biodiversity Outlook 3. Scenario Synthesis", Université Paris-Sud 11.

Leemans, Rik, "Applying global Change Scenarios to Assess Changers in Biodiversity", Bilthoven, 1999.

Litvinovitch, Jutta and Björn Ingendahl, "Klimawandel, Extremwetterereignisse und Gesundheit", Konferenzbericht, Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU), 2010.

Meijl, H. van, T. van Rheenen, A. Tabeau and B. Eickhout, "The impact of different policy environments on agricultural land use in Europe", Agriculture, Ecosystems and Environment 114, 21–38, Bilthoven, 2006.

Meyer, Rolf, Martin Knapp and Mathias Boysen, "Diskursprojekt „Szenario-Workshops: Zukünfte Der Grünen Gentechnik", Karlsruhe Institut für Technologie (KIT) and Bundesministerium für Bildung und Forschung (BMBF), 2009.

Millenium Ecosystem Assessment, "Ecosystems and Human Well-being: Biodiversity Synthesis", World Resources Institute, Washington, DC, 2005.

Mouysset, L., L. Doyen and F. Jiguet, "Different policy scenarios to promote various targets of biodiversity", 2011. http://www.elsevier.com/locate/ecolind

Mulugeta, Genene, Samuel Ayonghe, Deolall Daby, Opha Pauline Dube, Francis Gudyanga, Filipe Lucio and Ray Durrheim, "Natural and Human-induced Hazards and Disasters in sub-Saharan Africa", ICSU Regional Office for Africa Science Plan, 2007.

Narvinger, Anders, Henrik Blomgren, Sigrun Hjelmquist, Thomas Korsfeldt, Lars Gunnar Larsson, Bruno Nilsson and Monica Ulfhielm, "Energy Foresight – Sweden In Europe", Synthesis and Summary, Royal Swedish Academy of Engineering Sciences, 2003.

Nelson, Gerald C., Mark W. Rosegrant, Amanda Palazzo, Ian Gray, Christina Ingersoll, Richard Robertson, Simla Tokgoz, Tingju Zhu, Timothy B. Sulser, Claudia Ringler, Siwa Msangi and Liangzhi You, "Food Security, Farming, and Climate Change to 2050, scenarios, results, policy options", International Food Policy Research Institute, 2010.

OECD, "Environmental Policy, Technological Innovation and Patents", OECD Studies on Environmental Innovation, 2008.

OECD, "How's Life? Measuring well-being", OECD Publishing, 2011. http://dx.doi.org/10.1787/9789264121164-en

OECD, "Mortality Risk Valuation in Environment, Health and Transport Policies", OECD Publishing, 2012. http://dx.doi.org/10.1787/9789264130807-en

OECD, "*OECD Compendium of Agri-environmental Indicators*", OECD Publishing, 2013. http://dx.doi.org/10.1787/9789264186217-en

OECD, "OECD Environmental Outlook to 2050. The consequences of Inaction", OECD Publishing, 2012. http://dx.doi.org/10.1787/9789264122246-en

OECD, "Towards Green Growth", OECD Publishing, 2011. http://www.oecd.org/dataoecd/42/39/48432900.pdf

OECD, "OECD-FAO Agricultural Outlook 2012-2021", OECD Publishing and FAO, 2012.

Pehnt, Martin, Dr. Lars-Arvid Brischke, Sirkka Jacobsen, Dr. Guido Reinhardt, Horst Fehrenbach, Regine Vogt and Jan Walter, "Erneuerbare Energien Innovationen für eine nachhaltige Energiezukunft", Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), 2011.

Pereira, Henrique M. et al., "Scenarios for Global Biodiversity in the 21st Century", Science, American Association for the Advancement of Science, Vol. 330, 10th December 2010, pp. 1496-1501.

Ryan, Lisa and Nina Campbell, "The Multiple Benefits of Energy Efficiency Improvements", International Energy Agency (IEA), 2012.

Sala, Osvaldo E., "Biodiversity across Scenarios", Chapter 10.

Sala, Osvaldo E., "Global Biodiversity Scenarios for the Year 2100", Science magazin, VOl287, 2000. www.sciencemag.org

Sala, Osvaldo E., "Potential Biodiversity Change: Global Patterns and Biome Comparison".

Sala, Osvaldo E., "Consequences of changing biodiversity", Macmillan Magazines Ltd, 2000.

Schöne, Florian, "Auswirkungen der Flächen- und Nutzungskonkurrenz auf die biologische Vielfalt in Deutschland. Maßnahmen zum Erhalt der Biodiversität in der Kulturlandschaft", Technikfolgenabschätzung – Theorie und Praxis, Vol. 17, No. 2, September 2008, pp.60-66.

Searchinger Timothy, "Use of U.S. Croplands for Biofuels Increases Greenhouse Gases Through Emissions from Land Use Change", 2008. www.sciencexpress.org

Secretariat of the Convention on Biological Diversity, "Projections of 21st century change in biodiversity and associated ecosystem services", CBD Technical Series No. 50, 2010.

Slingenberg, Allister, Leon Braat, Henny van der Windt, Lisa Eichler and Kerry Turner, "Study on understanding the causes of biodiversity loss and the policy assessment framework", European Commission, Directorate-General

for Environment, Rotterdam, 2009.

Sofian-Azirun, M. and Y. Norma-Rashid, "Biodiversity Conservation and Sustainable Use: Malaysian Scenario", University of Malaya.

Spangenberg, Joachim H., "Scenarios for investigating risks to biodiversity", Global Ecology and Biogeography, Vol. 21, 2012, pp. 5-18.

Sullivan, Kathryn, "Global Biodiversity Indicators: scenario modelling for fisheries policy", London, 2010.

The Royal Society, "Measuring biodiversity for conservation", London, 2003.

Tigner, Brooks, Ramona Kundt, Octávia Frota, Alexander Siedschlag, Andrea Jerković, Susanne Kindl, Tudor

Tagarev, Juha Ahokas, Juha Hintsa, Diego Fernandez Vazquez and Rahel Suissa, "Thematic scenario portfolio (Work Packages 3-7) with reference scenarios for 'Security Research 2035'. Deliverable 8.1", Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles, Seventh Framework Programme, 2012. http://www.focusproject.eu/documents/14976/78b744e5-9daa-432b-be3b-92316416aa65

Turner, B. L., II, William B. Meyer and David L. Skole, "Global Land-Use/Land-Cover Change: Towards an Integrated Study", 2009.

United Nations Development Programme (UNDP), "Importance of Biodiversity and Ecosystems in Economic Growth and Equity in Latin America and the Caribbean: An Economic Valuation of Ecosystems", 2010.

United Nations Environment Programme (UNEP), "Global Environment Outlook 4", 2007.

United Nations Environment Programme (UNEP), "Securing Sustainability Through the Conservation and Use of Agricultural Biodiversity", Division for the Global Environment Facility, 2010.

University of Natural Resources and Life Sciences (BOKU), "Problem space report: Natural disasters and global environment change. Deliverable 4.1", Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles, Seventh Framework Programme, 2012.

Willis, Kathy, "Biodiversity futures: Scenario setting using lessons from the past", World Forum on Enterprise and the Environment, 2011.