D4.3 Focus group report

Deliverable submitted in April, 2013 (M16) in fulfilment of the requirements of the FP7 project, ETTIS – European security trends and threats in society

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

ETTIS	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:	**D4.3**
Title:	**A summary report on the findings made through the focus group**
Due date:	**29 February 2013**
Actual submission date:	**22 May 2013**
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 Institute for Systems and Innovation Research ISI
Erduana Shala, Fraunhofer Institute for Systems and Innovation Research ISI
Antje Bierwisch, Fraunhofer Institute for Systems and Innovation Research ISI

CONTENT

FIGURES

TABLES

EXECUTIVE SUMMARY

The overarching aim of the WP4 is the development of threat scenarios across different contexts in three domains: cyber infrastructure, nuclear material and environment as a basis for identifying societal needs. Scenarios provide an in-depth analysis of the key threats; they describe the relevant future developments and events and identify the main actors and their motivations. The developed scenarios help us to identify future possibilities, which are solutions and options related to societal needs.

There research work in WP4 is 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 4.3-4.5 "Scenario development and identifying societal needs".

The **interviews with key stakeholders** (task 4.1, see D.4.1) provide us with input regarding current and future threats and societal needs in the three mentioned domains. The first insights supported first the setting a thematic focus in each of the three domains and second deriving the key factors (most important aspects) for the development of the scenarios. The interview partners represent conventional security research end-users as well as public and civil society organizations engaged in societal needs on a general level. Apart from the interviews we analysed reports and deliverables of recently completed projects which have a similar focus as ETTIS. Thereby we want to make sure that we are not duplicating or even reemphasizing their results.

The main goal of the **text mining** (task 4.2, see D.4.1) was to identify possible future threats on the internet. 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 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.

The aim of the **scenario development** (tasks 4.3-4-5) is to develop the scenarios and to identify the societal security needs. This includes the analysis of the future studies within the domains cyber infrastructure, nuclear and environment as well as conducting focus groups workshops, which are described in this report. These results delivered the first input to the identification of threats and trends, which are the basis for the development of scenarios as well as to a deeper understanding of the contexts of the scenarios.

In order to identify different societal security needs WP4 will consider a number of ***threat scenarios*** in three different domains and across different ***context scenarios***. The selected domains for reflecting security trends and threats are cyber infrastructure, nuclear and environment.

Scenarios describe relevant future developments and offer different future perspectives for identifying future option spaces. They help us to identify the main actors and their motivations as well as future possibilities which are solutions and options related to societal security needs.

The scenario development within WP4 proceeds via two steps: In the first step context scenarios will be created, followed by the second step - the creation of threat scenarios. 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 ***contextual key factors*** have an overarching relevance for the field of security (e.g. EU policy, demography, trends and drivers in technology) and are equally important for the domains cyber infrastructure, nuclear and environment. The context analysis also includes the identification of emerging trends and global developments. The ***threat related key factors*** 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 focus groups (task 4.3) deliver input to the identification of threats and trends and to the development of scenarios as well as to a deeper understanding of the contexts of the scenarios. In order to build the basis for the scenario development the focus groups contribute firstly to the identification, discussion and prioritising of the key factors which influence and shape security in general as well as the selected domains today and in the future. Secondly they provide crucial and solid groundwork for identifying so called ***future projections***, which describe different possible future developments of the 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 are identified for contextual as well as for threat related key factors.

Based on the results of the focus setting within the originally broad defined domains (described in D4.1) experts of the following fields were invited to attend the focus groups workshops:

- 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.
- The focus group workshop for the domain environment should primarily focus 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.

The first focus group workshop on the future of cyber infrastructure was convened on the 13th and 14th November 2012. Based on the lessons learned from this workshop the two other focus group workshops were planned on the 27th and 28th November. However only the focus group workshop for the domain nuclear has been carried out and the focus group workshop for the domain environment had to be cancelled, since the number of confirmations wasn´t sufficient. At the beginning of November a new date for the workshop was set and the second invitation round started. We invited more than 90 experts and got a highly positive feedback to the importance of this topic and many offers of support for

scenario development. However we got only few confirmations of participation for the fixed dated workshop. As a substitution we restructured the 3rd focus group workshop to a combination of expert interviews and a survey. Accordingly, a comparable qualitative input of expert opinion and knowledge as for the other domains will be ensured.

The most important step of preparing the focus group workshops was 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 (see chapter 2). Regardless of the domain a broad range of different aspects from the following fields are frequently named: EU policy, EU development, socio-cultural developments, trends and drivers in technology, research landscape, ecology and sustainability or economy. However there are 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).

1 OBJECTIVES AND UNDERLYING DATA

The focus group workshops should deliver inputs at different stages of the process: to the development of scenarios, to the identification of threats, trends and needs as well as to a deeper understanding of the contexts of the scenarios. They should contribute to the process of identifying the different key factors and creating the future projections.

In general focus group research involves organised discussion with a selected group of individuals to gain information about their views and experiences of a topic. Focus group interviewing is particularly suited for interaction with experts and obtaining several perspectives about the same topic. One focus group for each field, cyber infrastructure, nuclear and environment was planned (see figure 1).

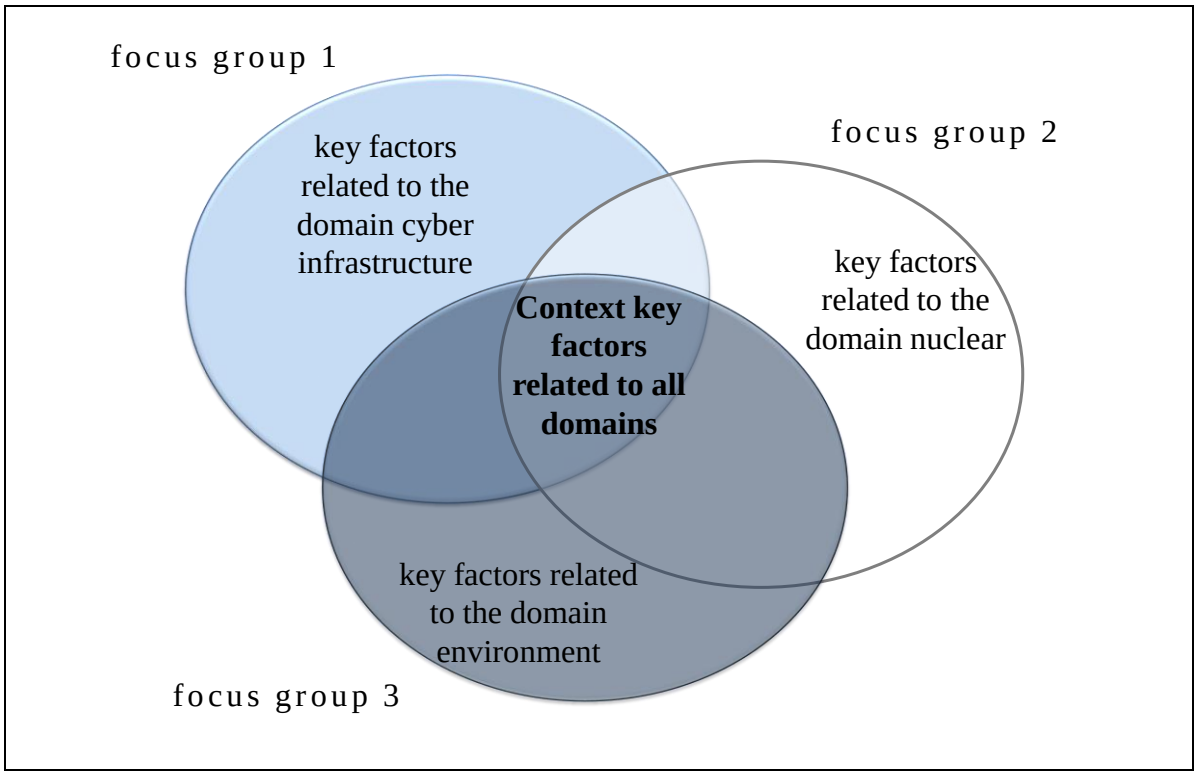
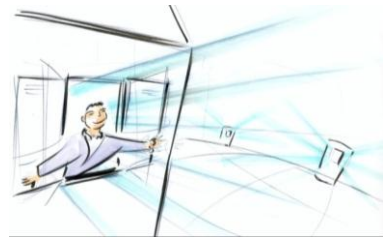


Figure 1: Discussing the key factors on context and domain level in focus groups (own illustration)

For this reasons we invited representatives of companies which deal with security in general, e.g. work in security businesses, develop or use security technologies as well as deal with further security aspects, like societal issues. For inviting persons, the desk research was used as well as the results from the interviews with key stakeholders.

The objectives for each focus group workshop are listed in the figure below (see figure 2). These objectives are embedded in the whole process of the scenario development.

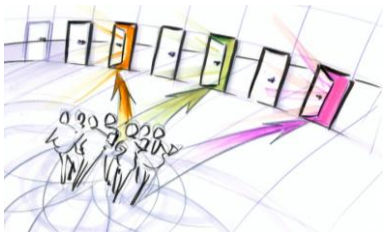


(1) Extend the perception: thinking beyond established pathways

- ✓ Future studies analysis in the considered field
- ✓ Expert identification and selection
- ➡ Identification and discussion of the relevant factors (✓)

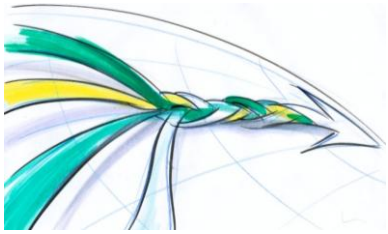
(2) Handling complexity: discuss the key factors separately

- ➡ Factor evaluation
- ➡ Factor selection for the further discussion



(3) Considering alternative developments for each key factor

- ➡ Identification id uncertainties (✓)
- ➡ Development of the future projections



(4) Bundling of possible developments: building of different scenarios with a high internal consistency

- ▪ Consistency check between the future projections
- ▪ Bundling the future projection to scenarios
- ▪ Scenario writing

Caption:
✓ achieved before the workshop ➡ to achieve during the workshop ▪ to achieve after the workshop
Illustrator: Heyko Stöber

Figure 2: Objectives of the focus group workshop (own illustration)

For preparing the focus group workshops, in particular the identification of the key factors, a wide range of sources was used, like various future studies and research works with focus on the future as well as the first findings from the tasks 4.1 (Interviews with stakeholders) and 4.2 (IT-based weak signal mining) as outlined in D4.1. Based on the desk research a wide range of future studies related to both context and the domains cyber infrastructure, nuclear and environment were collected. Additional the findings of task 2.2 were used, which provide an in-depth analysis of the key trends emerging from completed and ongoing foresight and other relevant security projects, undertaken both in Europe and beyond.

We analysed almost 300 documents which provide descriptions of different futures related to various aspects from the field of security in general as well as cyber, 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:

- What are the most important aspects characterising and influencing the field of security today and in the future?
- What are the most important aspects characterising and influencing the domains cyber infrastructure, nuclear and environment?
- What are the present developments of these aspects?
- What are possible developments of these aspects?
- Are there different developments of the same aspect?

The first and the second question aim at finding key factors by analysing the aspects described in the future studies. Mostly, aspects that are similar may also be summed up and considered as one key factor. For example, different societal and political aspects concerning the development of the EU might be summed up to a key factor named "societal and political development of the EU" (like in table 1). The next step is to capture the situation today and possible future projections of the certain aspect that are given in the literature. In order to answer these questions and structure the stocktaking of the key factors and future projections we used a template structured as follows:

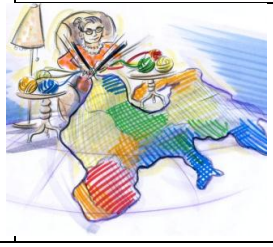
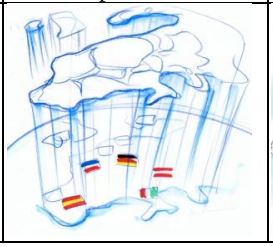
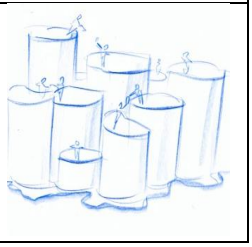
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Societal and political development of the EU	The integration of the EU is seen primarily as a political process: • The 27 members of the EU are difficult to integrate • The Treaty of Lisbon does not provides the desired effects • The consolidation of the Greek state budget is a major test for the EU Monetary Union	Strong development of Europe: • The Treaty of Lisbon has positive effects • There is an European consensus on security and CO2 reduction • Integrated business and work space • People feel connected with Europe as the European citizens	Europe of different regions (medium development): • Europe of different regions with the appropriate constitution, etc. • Most activities have their focus on the regions, national level rather unimportant	Return to the interests of their own nation and region: • The EU is no longer capable of making decisions • It is difficult to cooperate related to the economic policy or foreign policy and other fields • monetary union is threatened by the bankruptcy of several states
				

Table 2: Exemplary description of a key factor (own compilation)
Illustrator:Heyko Stöbber

For each domain as well as for the context the identified aspects were clustered to several main groups under a higher level heading. The aspects built the base for the discussion in focus group workshops (see table 2-5 below), where they were discussed and prioritized (see chapter 2).

EU-Policy and Development	International Policy Environment	Socio-cultural Developments	Demographic Change	Trends and Drivers in Technology	R&D Characteristics	Ecology and Sustainability	Stability, Complexity and Resilience	Economy	Labour and Production Models	Relevant Sectors
• institutional development (legitimacy, confidence) • shaping world developments, global foreign policy issues • transnational security • financial crisis • innovation system • regulation	• security policy (international, human) • internationalization of economic policy • trade embargos, protectionism • defense (military power, frontier disputes, deterrence, militarization of space) • fiscal imbalances (like public debt)	• attitude towards new technologies • shift in political beliefs (social and religious tensions, radicalization) • work life balance values • societal inequality (social tensions, wealth concentration) • shifting cultural and social influences (e.g. from Americanization to Asian cultural influences) • sustainable society • urbanization vs. rural population • attitude towards organized crime, corruption • traditional and virtual communities (social networks, digital identity)	• aging society, low fertility rate, shrinking population • migration, immigration (policy)	• technology development (decrease, stagnation, growth) • disruptive technologies • convergence & interoperability • user acceptance • interconnection of technologies	• balance of institutional participation, e.g. EU, universities, research institutes, enterprises • commercialization strategy • interdisciplinary & networking • innovation systems • research governance • providing information to society • bias / focus of research areas • IPR, open source	• growth of sustainability • population growth • housing • renewable energy • exploitation of natural resources • water supply	• terrorism • (global) economic situation (recession, crisis, breakdown) • resource scarcity • deterrence (e.g. weapons of mass destruction, arms race) • autocratic and authoritarian political systems (instability sources, critical systems) • humanitarian emergencies • governance architecture	• consumption • economic policy (competition policies, types of competition) • shifting power and balances (e.g. the Asian Meridian) • relations & alliances between politics and business • reversal of economic globalization • economic crime • extent of service sector • manufacturing productivity • geopolitics • international cooperation	• new production models (work flow etc.) • changing realities in labor markets, virtuality • highly qualified workers	• energy • food • health • …

Table 3: Relevant aspects for the context (own compilation)

Technology	Research Landscape	Attack Targets, Vulnerability	Societal Developments	Protection Responsibility	Markets	Attacker Forms/ sources and Types of Attacks	EU-Policy	Education and Skills	Relationships, Impact
• parameters (bandwidth, processing power, …) • cloud computing • Internet platforms • compatibility software and hardware • ICT connectivity • network architecture • strengths and weaknesses of software • protection technologies: access, identity check, firewalls, encryption • trustworthy data exchange • design "to" security • fraud detection	• industry / private sector / research institutions • private sector • research institutions • funding • cyber security strategy (research strategy) • interdisciplinary & cross-sectoral research • push vs. pull (consumption behavior)	• financial institutions (e.g. financial flows) • server & data storage • critical infrastructures • mobile phones & mobile networks • social networks • IT based services (i.e. smart grids, cloud computing) • IT-networks (e.g. governments, companies) • human factor	• security understanding, perception of protection • education/ growing IT-skills • handling the data / data retention • use of internet platforms & web services • privacy of & trust in • social networks • internet access & mobile networks • user competence • working flexibility (IT-necessity) • digital natives/net-work society	• private / public / governmental duty • perception of protection necessity • education / providing with information (private vs. companies) • scale of cyber security • public or private security, e.g. rail stations • commitment / cooperation related to action • control and protection against enemy cyber attacks • protection institutions, safeguards • investments in security and network architecture	• supply vs. demand of cyber technologies • use of cyber space by different players (e.g. E-governments, companies, individuals) • competition • globalization • quality of data / information • cyber as an economical sector (market structures / products) • digitalization in / of cultural institutions and archives	• hostile states, cyber warfare • criminals • terrorists • hacker activists • cyber espionage • theft of data	• criminal prosecution • privacy / data security • harmonization, standardization • policy flexibility • regulatory framework (prevention and protection, legal data protection) • traceability • cyber security & strategy	• transformation of knowledge (lifelong learning, new learning methods & environments) • infrastructure investments • talents & highly qualified (recruiting processes) • use of media (interactive / collaborative / abuse)	• attacks impacts: on security; on counter-measures • cascading influence • financial damages • insurances • survivability • economic of information security • energy as a target as well as a basis for IT-infrastructure • virus: shift from technology protection to attack technology

Table 4: Relevant aspects for the domain cyber infrastructure (own compilation)

Quantities & Infrastructure	Material Control and Accounting Procedures	Handling of Disposal and Transport	Global Norms (legal framework)	Societal Factors	EU-Policy	Research and Technology Progress	Human Resource Factor	Protection Responsibility
• quantities of nuclear materials • number of sites • types of nuclear materials • energy mix • frequency of materials transport • materials production / elimination trends • emergency response capabilities • nuclear infrastructure protection plan • structure of the supporting nuclear industry infrastructure • nuclear as an economical sector (market structures/ products, development)	• regulatory framework conditions • measurement methods • inventory record • materials balance areas • management interdependencies • control of radioactive waste generation	• physical security during transport • types of storage • misuse • reprocessing • reliability host material	• international legal commitments • voluntary commitments • nuclear security and materials transparency • national legal framework	• security understanding and concerns & perception of protection • user awareness of threats • political stability (social unrest, international disputes or tensions, armed conflict) • pervasiveness of corruption • groups interested in illicitly acquiring materials • human health issues • adoption of new technology	• criminal prosecution • policy flexibility • regulatory framework (trend: increase, decrease) vs. self regulation • harmonization of regulations • taxes	• industry / private sector / research institutions • financing / funding • interdisciplinary & cross-sectoral research • push vs. pull (consumption behavior) • research based on societal needs	• skills (security personnel vetting, performance demonstration) • certification • talents & highly qualified (recruiting processes) • infrastructure investments	• private / public / governmental duty (PPP) • perception of protection necessity • education / providing with information • safeguards adoption & compliance • institutional setting (independent regulatory agencies)

Table 5: Relevant aspects for the domain nuclear (own compilation)

Societal Factors	EU-Policy	Research and Technology	Resources and Sustain-ability	Climate change	Economy	Agriculture	Forestry	Land Use	Species and Habitat	Water and Marine
• demography • urbanization vs. rural population • labor • tourism • human behavior, lifestyle • adoption of technology • education and skills • consumption • importance of healthy environment • social wealth • impacts of human activities on environment • relationship between deaths and environment (issues in general)	• pest control and disease regulation • energy policy • mitigation policy • environmental policy • EU chemicals policy: REACH • EU common agricultural policy • integrity social, environmental and economic policy • handling the complexity of the food web • EU strategy for biodiversity management • policy options and their effects on future land cover distributions • fields of regulation and deregulation • EU funds • geopolitics and international cooperation • measure methods • conservation status of a natural habitat	• sustainable technologies • technological development (innovations) • efficiency of ecosystem • modern crop varieties (energy crops)	• ecoregions • complexity of and changes in ecosystems • fossil fuels • renewable energy sources • exploitation of natural resources • global biogeochemical cycles • development of ecological and environmental sciences • productivity and sustainability	• atmospheric CO2 concentration • changes in climate • impact of climate change • pollution (air and water purification) • nitrogen deposition, acid rain • changes in abiotic conditions, surface albedo, ocean acidification, precipitation • rise of temperature • meteorology-cal conditions	• development rate • infrastructure development • degree of globalization • demand on natural resources • energy sector • major market failure • commercialization • investment fund for green business • factor productivity improvements • international cooperation • institutional factors • rates of crop yield	• agriculture development • food and agriculture production • chemical use and pollutants • waste and material flows • use of organic fertilizers • soil structure, fertility and conservation • relationship of forest and agricultural systems • agronomy • influence of soil and water pollution • biomass • linking of industrial, energy and agricultural activities	• European forest area • fire resilience • global forest area • wood exploitation (timber extraction, wood-fuel)	• eutrophica-tion • type of use/ land conversion • soil structure (land degradation, acidification, land clearance resulting in loss of primary habitat and soil fertility) • recreation (cultivation, grazing, survival through chemical and mechanical treatments) • security of land tenure, land availability	• biotic exchange and interactions • Stock of natural habitats, biotope size • species biodiversity • introduction of invasive species, invasive alien species • exploitation of species • reproduction (vegetation, pollination loss, phytoplankton productivity, gender equity) • biological pollution • coral reef building	• flood protection measures • hydrological cycles, measures and services • precipitation rate • water and resource availability and use • water characteristic • exploitation in marine ecosystems • diversion of water to intensively managed ecosystems and urban systems • development rivers • diversity of marine biomass • fisheries

Table 6: Relevant aspects for the domain environment (own compilation)

2 APPROACH OF THE FOCUS GROUP WORKSHOPS

The focus group workshop approach was chosen in order to support active participation and the dialogue of experts from different interested groups. The discussions focus on different future developments in a particular area based upon the partcipants' own experiences. The workshop process is a combination of different moderated activities, brainstorming as well as input presentations. The optimal group size is 8-12 participants. The same experts may also meet several times ("panel" approach).

The key characteristics of the focus groups are:

- working out of the thematic focus on a specific (future) issue,
- in-depth discussion of (future) issues,
- working out of a structured content,
- development of recommendations,
- but: no decision making; decisions are often performed elsewhere.

The focus group workshops within WP4 were in each case two-day events. They started with an introductory session in plenary, welcoming the participants and providing them with information concerning the project and the time schedule of the workshop. The general issues related to the project and the methodology of the workshop, as well as the expectations of the hosts were discussed. In return the participants provided information about their profession, the organisation they represent and their motivation in attending the workshop. After the introducing part some participants presented their own view on the relevant aspects in the referred domain and shared their experiences in order to inspire the attendees and set a basis for the further discussion. The focus of the further work was on identifying, prioritising and discussing the key factors and their future projections. The discussions have been carried out in small groups followed by the presentation of the group findings and discussion in plenary sessions. The workshop was finalised with a summary of the results of the workshop and a feedback from the participants in order to find out if their expectations have been met (see figure 3).

The focus group workshops were an important step to ensure end-user engagement throughout the scenario development. A total number of 22 participants attended the focus group workshops, including 12 end-users and representatives of research institutes as well as the European Commission.

The first focus group workshop on the future of cyber infrastructure took place on the 13th and 14th November 2012. Based on the lessons learned from this workshop the two other focus group workshops were planned on the 27th and 28th November 2012. However only the focus group workshop for the domain nuclear has been carried out whereas the focus group workshop for the domain environment had to be cancelled since the number of confirmations was not sufficient. At the beginning of November 2012 a new date was set and the second invitation round started. We invited more than 90 experts and got a highly positive feedback to the importance of this topic and many offers of support for scenario development, however we got only few confirmations of participation for the fixed dated workshop (on the 30th and 31st January 2013).

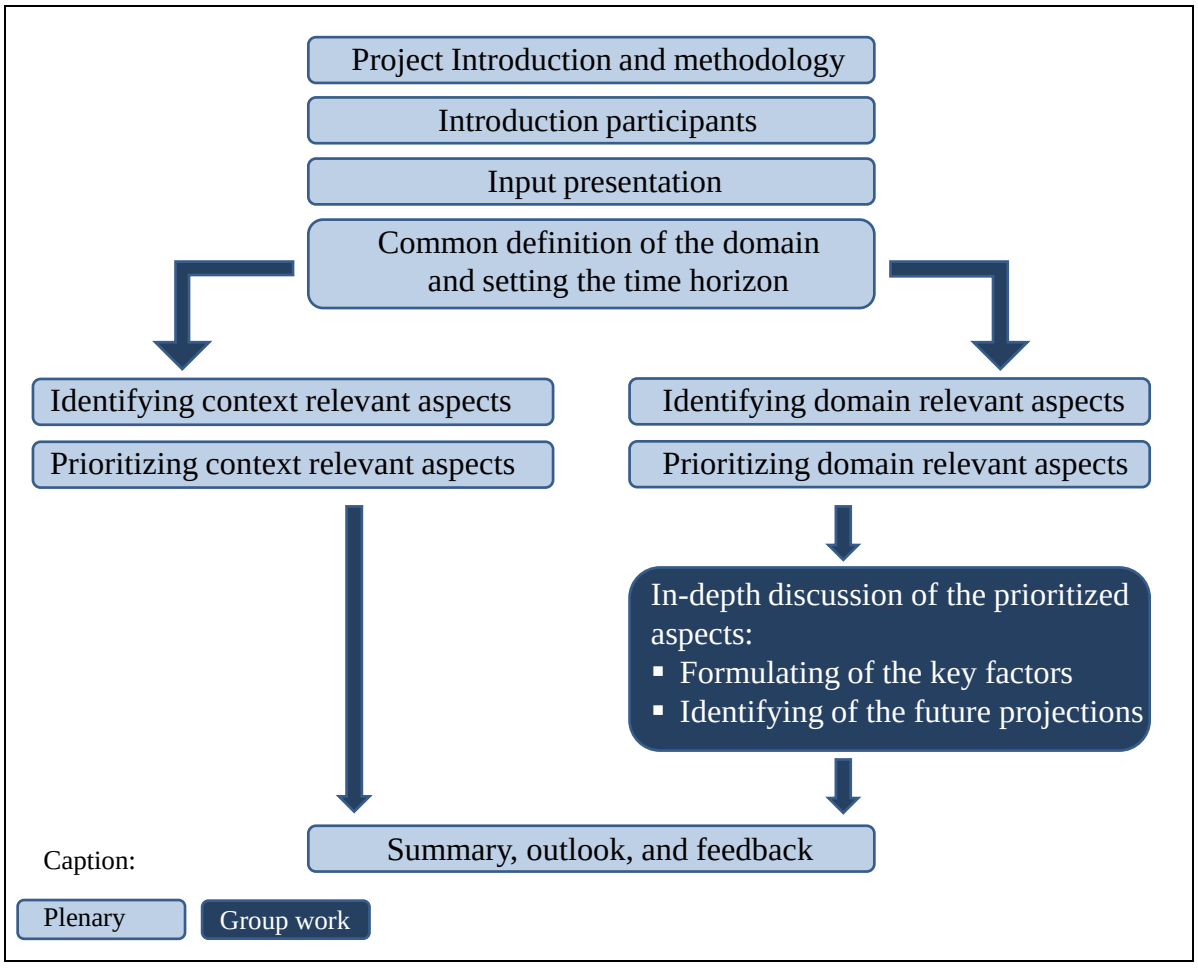


Figure 3: Schematic presentation of the focus group workshop approach (own illustration)

An important topic on the agenda was discussion of the time horizon. 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.

2.1 FINDINGS OF THE WORKSHOP ON CYBER INFRASTRUCTURE

The cluster with aspects relevant for context and the domain cyber infrastructure, which build the base for the discussion in focus group workshop overlap – hence they could be useful for linking the context and domain scenarios (see figure 4 below).

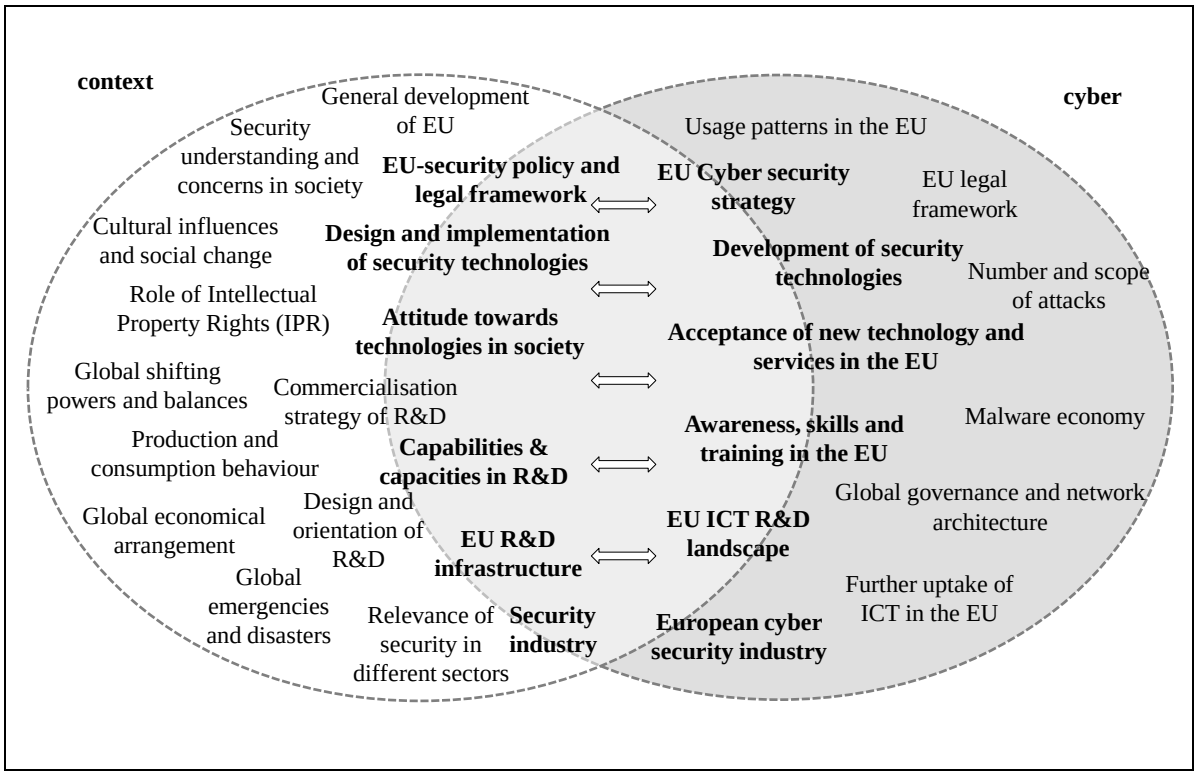


Figure 4: Overlaps between context and cyber infrastructure (own illustration)

2.1.1 Context

Based on the contextual aspects presented in the table 2 (see white sheets, tables 6 to 16) the experts discussed and added further relevant aspects (see yellow cards). Subsequent work was to prioritize the most important aspects regarding the following criteria:

- Relevance for the future (time horizon 15-20 years)
- Relevance for the EU
- Relevance for security
- Relevance for the society
- Relevance for the domain cyber infrastructure

The following caption applies to tables 6 to 16:

Aspects gained from the key factor stocktaking *Aspects gained from the experts input in workshop* * Prioritized by experts (one * per person)

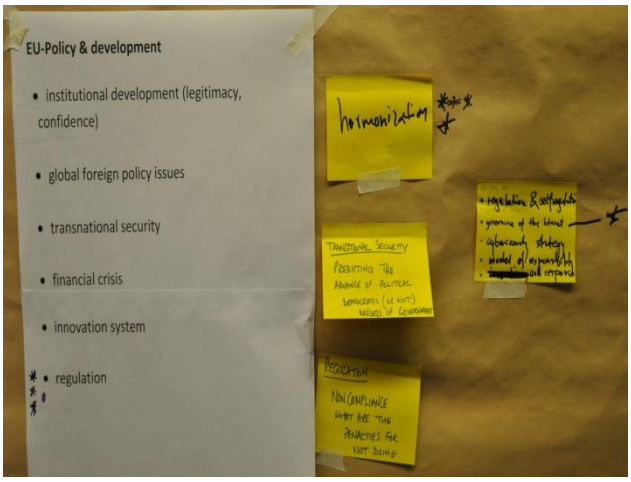
	• institutional development (legitimacy, confidence) • global foreign policy issues • transnational security • *predicting the advance of political democratic (or not) models of government* • financial crisis • innovation system • regulation **** • *compliance, what are the penalties for not doing* • *harmonization* **** • *regulation & self-regulation* • *governance of the internet* * • *cyber security and strategy* • *model of responsibility and response*

Table 7: Factor evaluation for context scenarios - EU-policy and development (own compilation)

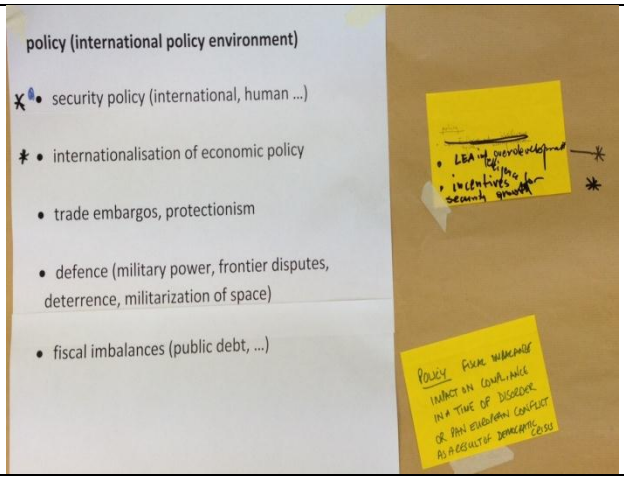
	• security policy (international, human …) ** • *LEA intelligence overdevelopment* * • *Incentives for security growth* * • internationalization of economic policy * • trade embargos, protectionism • defence (military power, frontier disputes, deterrence, militarization of space) • fiscal imbalances (public debt, …) • *impact on compliance in a time of disorder or Pan-European conflict as a result of democratic crisis*

Table 8: Factor evaluation for context scenarios - International policy environment (own compilation)

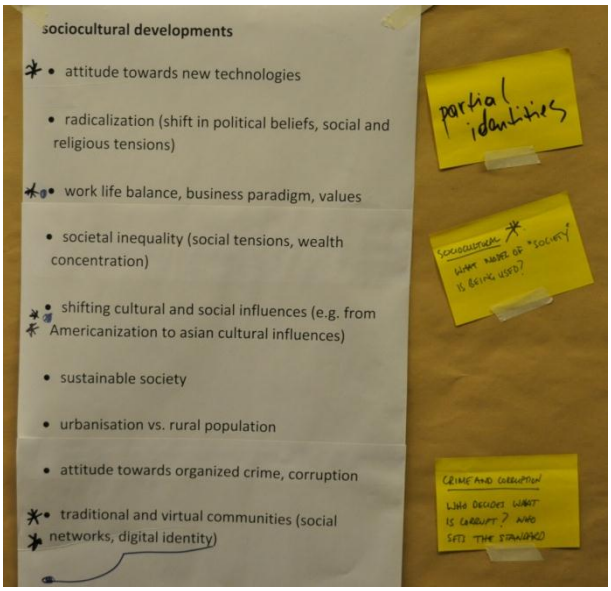
	• attitude towards new technologies * • radicalization (shift in political beliefs, social and religious tensions) • work life balance, business paradigm, values ** • societal inequality (social tensions, wealth concentration) • shifting cultural and social influences (e.g. from Americanization to Asian cultural influences) ** • sustainable society • urbanization vs. rural population • attitude towards organized crime, corruption • traditional and virtual communities (social networks, digital identity) *** • *partial identities* • *socio-cultural – what model of 'society' is being used* * • *crime & corruption – who decides what is corrupt?* *who sets the standard?*

Table 9: Factor evaluation for context scenarios - Socio-cultural developments (own compilation)

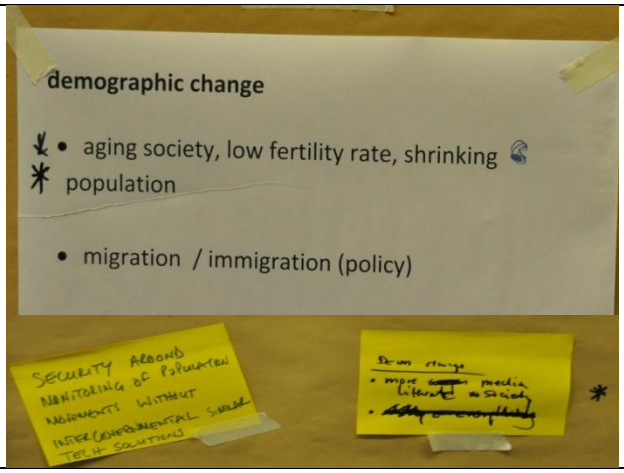
	• aging society, low fertility rate, shrinking population *** • migration / immigration (policy) • *security abound, monitoring of population movements without intergovernmental similar tech solutions* • *more media literate society* *

Table 10: Factor evaluation for context scenarios - Demographic change (own compilation)

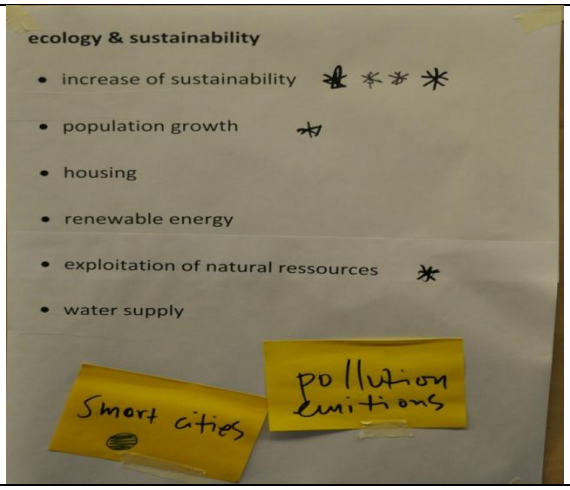
	• increase of sustainability *** • population growth * • housing • renewable energy • exploitation of natural resources * • water supply • *smart cities* * • *pollution emissions*

Table 11: Factor evaluation for context scenarios - Ecology and sustainability (own compilation)

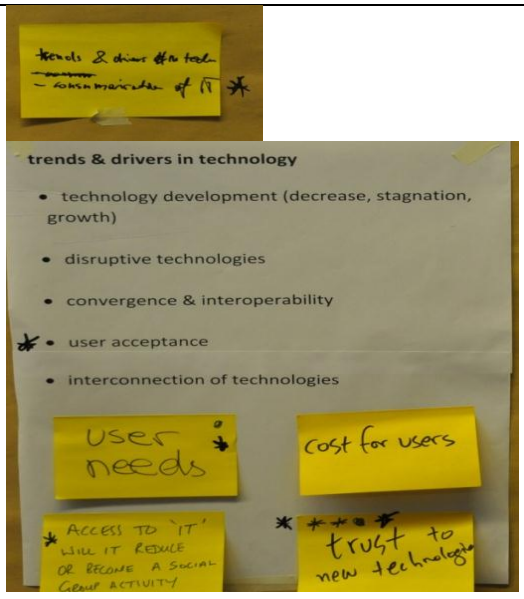
	• technology development (decrease, stagnation, growth) • disruptive technologies • convergence & interoperability • user acceptance * • interconnection of technologies • *user needs* ** • *cost for users* • *trust to new technologies* ***** • *access to 'IT' will reduce or become a social group activity* * • *Consumerisation of IT* *

Table 12: Factor evaluation for context scenarios - Trends and drivers in technology (own compilation)

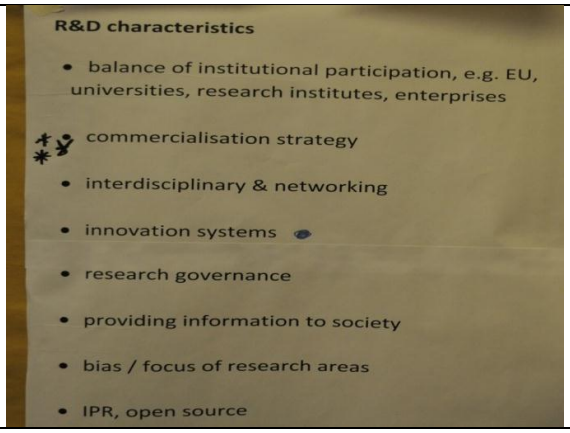
	• balance of institutional participation, e.g. EU, universities, research institutes, enterprises • commercialization strategy *** • interdisciplinary & networking • innovation systems * • research governance • providing information to society • bias / focus of research areas • IPR, open source

Table 13: Factor evaluation for context scenarios - R&D characteristics (own compilation)

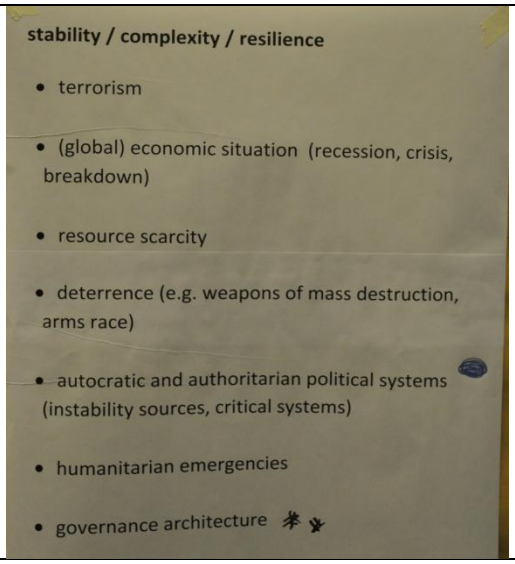
	• terrorism • (global) economic situation (recession, crisis, breakdown) • resource scarcity • deterrence (e.g. weapons of mass destruction, arms race) • autocratic and authoritarian political systems (instability sources, critical systems) * • humanitarian emergencies • governance architecture **

Table 14: Factor evaluation for context scenarios - Stability/ complexity/ resilience (own compilation)

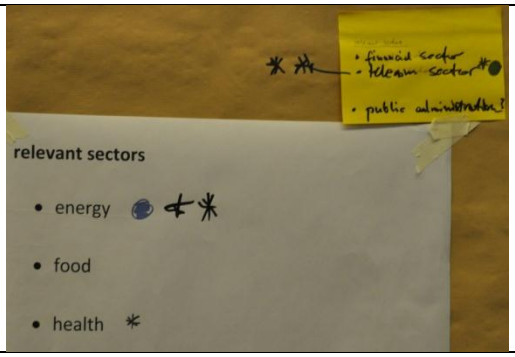
	• energy *** • food • health * • *Financial sector* • *Telecommunication* **** • *public administration*

Table 15: Factor evaluation for context scenarios - Relevant sectors (own compilation)

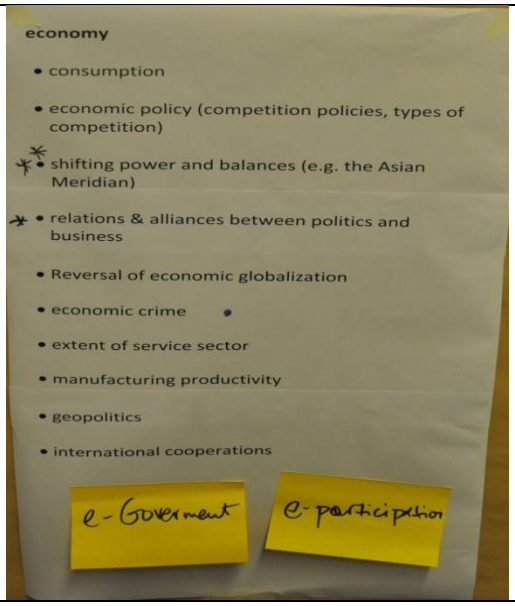
	• Consumption • economic policy (competition policies, types of competition) • shifting power and balances (e.g. the Asian Meridian) ** • relations & alliances between politics and business * • reversal of economic globalization • economic crime * • extent of service sector • manufacturing productivity • geopolitics • international cooperation • *e-Governance* • *e-Participation*

Table 16: Factor evaluation for context scenarios - Economy (own compilation)

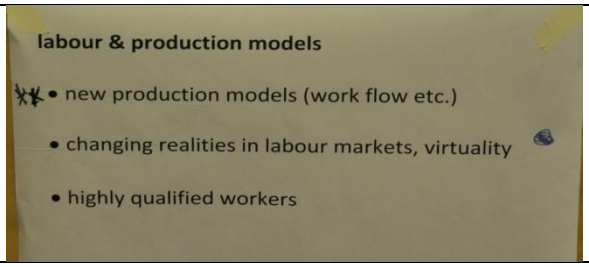
	• new production models (work flow etc.) ** • changing realities in labour markets, virtuality * • highly qualified workers

Table 17: Factor evaluation for context scenarios - Labour & Production Models (own compilation)

2.1.2 Cyber infrastructure

Based on the contextual aspects presented in the table 3 (see yellow cards, tables 17 to 26) the experts discussed and added further relevant aspects (see orange cards). Subsequent work was to prioritize the most important aspects regarding the following criteria:

- Relevance for the future (time horizon 5-10 years)
- Relevance for the EU
- Relevance for security
- Relevance for the society

The following caption applies to tables 17 to 26:

Aspects gained from the key factor stocktaking *Aspects gained from the experts input in workshop* * Prioritizing by experts (one * per person) **Detailed discussion** (formulating key factors and future projections)

	• industry / private sector / research institutions • private sector • research institutions • funding • Cyber security strategy (research strategy) * • Interdisciplinary & cross sectoral research • push vs. pull (consumption behavior) • Predictability models possible? *

Table 18: Factor evaluation for domain cyber - Research landscape (own compilation)

	• **security understanding, perception of protection **** • ***User awareness of threads*** • ***Privacy as right **** • **privacy of & trust in social networks** • Education/ growing IT-skills • handling the data / data retention • *Data detection* • use of internet platforms & web services • internet access & mobile networks • user competence • working flexibility (IT-necessity) • digital natives/network society * • *Mobile use of internet (mobile networks)* * • Dependence of IT-networks

Table 19: Factor evaluation for domain cyber - Societal developments (own compilation)

	• General Computing Capacities (bandwidth, processing power, …) • cloud computing • Internet platforms • compatibility software and hardware • ICT connectivity * • network architecture • Internet access & mobile networks * • Mobile wallets • strength and weaknesses of software • protection technologies: Access control, Identity check, Firewalls, encryption *** • Personal sensors (e.g. mobile phones as sensors) • Identity Management * • trustworthy data exchange • design "to" security * • fraud detection • crosslinking of technologies

Table 20: Factor evaluation for domain cyber - Technology (own compilation)

	• transformation of knowledge (lifelong learning, learning methods & environments) ** • infrastructure investments • talents & highly qualified (recruiting processes) • use of media (interactive / collaborative / abuse) • certification *

Table 21: Factor evaluation for domain cyber - Education and skills (own compilation)

	• **supply vs. demand of cyber technologies *** • **use of cyber space by different players (e.g. E-governments, companies, individuals) *** • **globalization** • **digitalization in/of cultural institutions and archives** • competition • **quality of data/ information** • **cyber as an economical sector (market structures / products) ***** • ***Charity and financial aid encouraging fiscal growth*** • internet as an economic factor • Economics of information security *

Table 22: Factor evaluation for domain cyber - Markets (own compilation)

	• hostile states, cyber warfare • **Criminals ***** • **cyber spies** • ***Underground economy*** • terrorists • hacker activists • **Theft of data *** • ***Identity theft ***** • *Accidental disclosure* • *Tracking (misuse of location based services) ** • *Linkability / profiling*

Table 23: Factor evaluation for domain cyber - Attacker forms, sources and types (own compilation)

	• **financial institutions (e.g. financial flows) *** • **critical infrastructures **** • **IT-networks (e.g. governments, companies)** • server & data storage * • mobile phones & mobile networks ** • social networks • IT based services (i.e. smart grids, cloud computing) • human factor * • Energy as a target as well as a basis for IT-infrastructure * • Cascading influence * • Financial damages *

Table 24: Factor evaluation for domain cyber - Attack targets and vulnerability (own compilation)

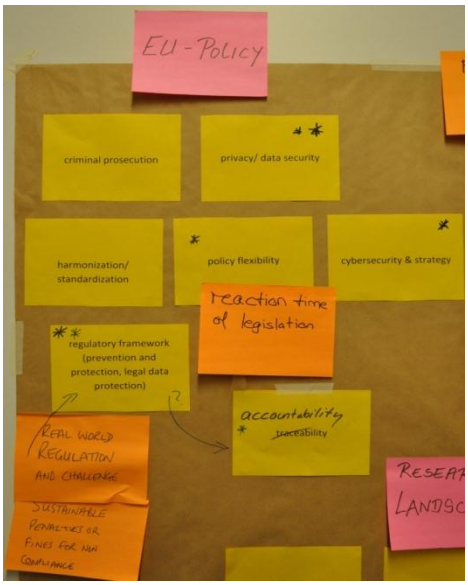
	• criminal prosecution • privacy/ data security + cyber security & strategy *** • harmonization/ standardization • policy flexibility • **regulatory framework (prevention and protection, legal data protection)** • ***Real world regulation and challenge ***** • ***Sustainable penalties or fines for non compliance*** • **(traceability)** ***accountability*** • *Reaction time of legislation **

Table 25: Factor evaluation for domain cyber - EU-policy (own compilation)

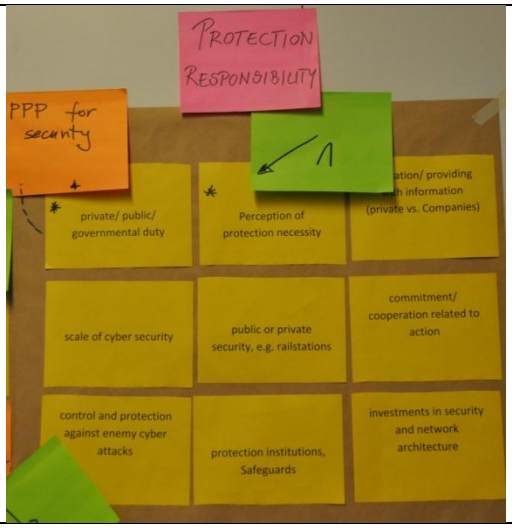
	• private/ public/ governmental duty * • *PPP for security* * • Perception of protection necessity * • education/ providing with information (private vs. Companies) • scale of cyber security • public or private security, e.g. railstations • commitment/ cooperation related to action • control and protection against enemy cyber attacks • protection institutions, Safeguards • investments in security and network architecture

Table 26: Factor evaluation for domain cyber - Protection responsibility (own compilation)

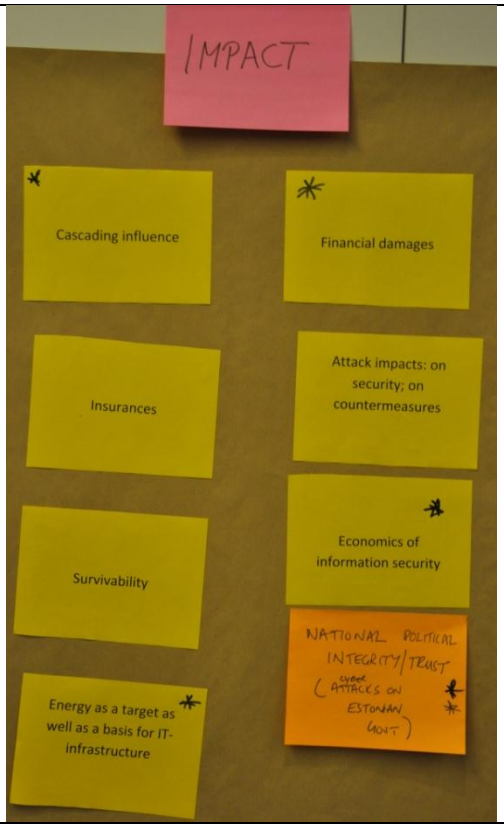
	• Attack impacts: on security; on countermeasures • Insurances • Survivability • Virus: shift from technology protection to attack technology • *National political integrity/trust (cyber attacks on Estonian government)*

Table 27: Factor evaluation for domain cyber - Impact (own compilation)

The focus of the further work was on identifying, prioritising and discussing the key factors and their future projections in small groups (see tables 28-34).

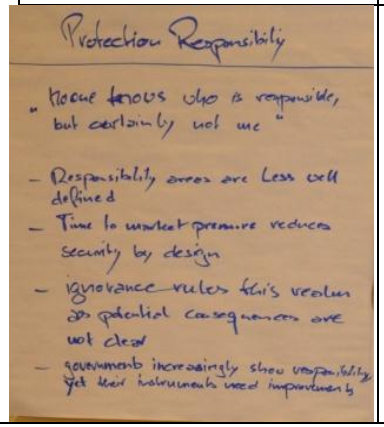
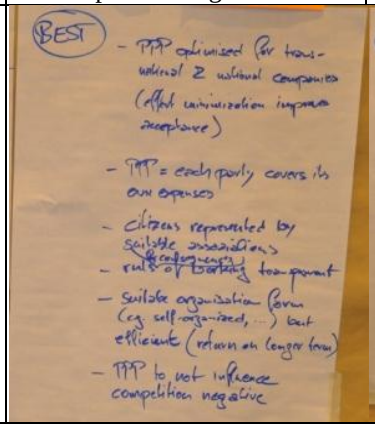
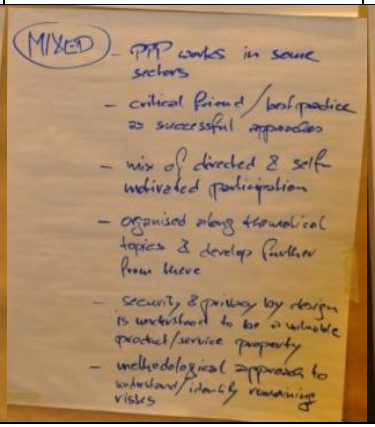
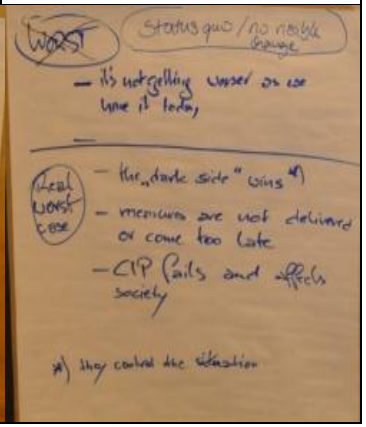
Key factor	Situation today	Future projection A	Future projection B	Future projection C	Future projection D
Protection responsibility	• Responsibility areas are less well defined • Time to market pressure reduces security by design • Ignorance rules this realm as consequences are not clear • Governments increasingly show responsibility yet, but their instruments need improvements	Status Quo/ Worst Case: • No visible change since today • It is not getting worse as we have it today	Best Case • PPP optimized for transnational & national companies (effort minimization improves acceptance) • PPP = each party covers its own expenses • Citizens are represented by suitable associations • Rules & consequences of working are transparent • Suitable organization form (e.g. self-organized) but efficient (return on longer term) • PPP do not influence competition negative	Mixed Case • PPP works in some sectors • Critical friend/best practice as successful approaches • Mix of directed and self-motivated participation • Organized along thematically topics and develop further from there • Security and privacy by design is understood to be a valuable product/service property • Methodological approach to understand/identify remaining risks	Real Worst Case • The „dark side“ wins (they control the situation) • Measures are not delivered or come too late • CIP fails and affects society
					

Table 28: Cyber key factors and future projections - Protection responsibility (own compilation)

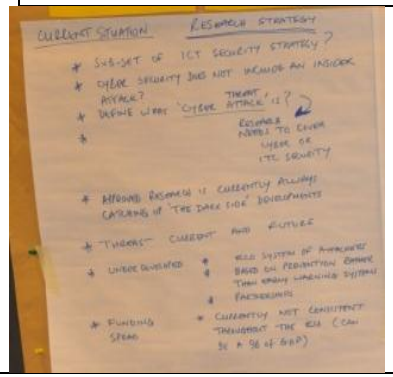
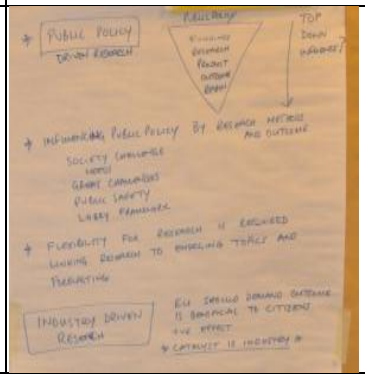
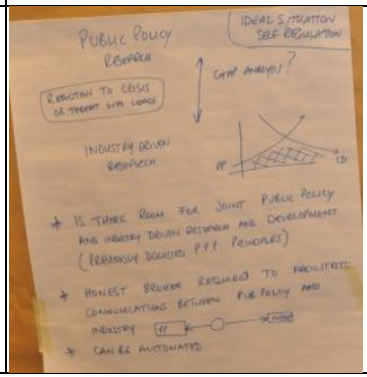
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Research strategy	• Subset of ICT security strategy? • Cyber security does not include an insider attack? • Define what 'cyber attack/threat' is • Research needs to cover cyber or ICT security • Approved research is currently always catching up 'the dark side' developments • Threats – current and future • Underdeveloped eco system of attackers/based on prevention rather than early warning systems/ partnerships • Funding spread; currently not consistent throughout the EU (can be a % of GDP)	Worst Case: • It is not getting worse as we have it today	Best Case • Public policy driven research (top-down influence?): funding-research-product-outcome-review • Influencing public policy by research methods an outcome (society challenge needs great challenges/public safety/ lobby framework/ • Flexibility for research is required, linking research to emerging topics and forecasting • Industry driven research: EU should demand, outcome is beneficial to citizens • the effect: Catalyst industry	Mixed Case • Public policy research or industry driven research (ideal situation: self-regulation) • Reaction to crisis or threat who leads • Is there room for joined public policy and industry driven research and development? (previously discussed PPP principles) • Honest broker required to facilitate communications between public policy and industry • can be automated
				

Table 29: Cyber key factors and future projections - Research strategy (own compilation)

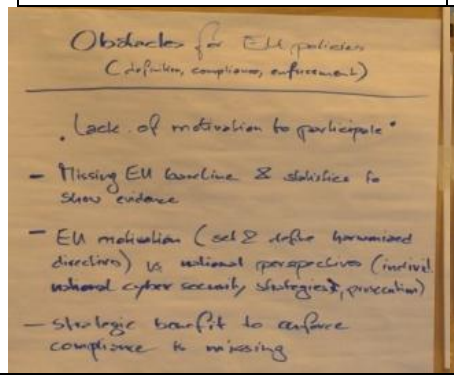
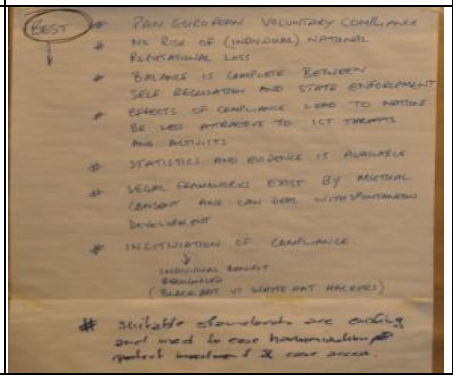
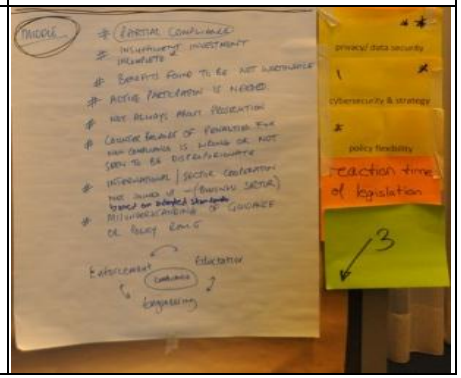
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Obstacles for EU policies (definition, compliance, enforce-ment)	• Missing EU baseline and statistics to show evidence • EU motivation (set & define harmonized directives) vs. national perspectives (individual cyber security, strategy, prosecution) • Strategic benefit to enforce compliance is missing	Worst Case: • No harmonization • EU directives ignored • National egoism • Widespread non compliance • Thread of international and international loss of life (transnational alliances) • Lack of cooperation on the international level • Role of cyber security is vital for the continued principles of the EU (fiscal policy in euro crisis is forced compliance and national agreements) • Legal frameworks slow → development of ICT fast → influenced by nationality • Lack of applicable standard or not using existing standards make any harmonization harder to achieve	Best Case • Pan-European voluntary compliance • No risk of (individual) national reputational loss • Balance is complete between self regulation an state enforcement • Effects of compliance lead to nations be less attractive to ICT threats and activists • Statistics and evidence is available • Legal frameworks exist by mutual consent and can deal with spontaneous development • Incitisation of compliance → individual benefit recognized (black hat vs. white hat hackers) • Suitable frameworks are enabling and used to ease harmonization, protect investment and ease access	Middle Case • Partial compliance • Incomplete or Insufficient investment • Benefits found to be not worthwhile • Active participation is needed • Not always about prosecution • Counter balance of penalties for non compliance is wrong or not seen to be disproportionate • International/ sector cooperation, not joined-up (Business sector), based on adopted standards • Misunderstanding of guidance or policy remote
				

Table 30: Cyber key factors and future projections - Obstacles for EU policies (own compilation)

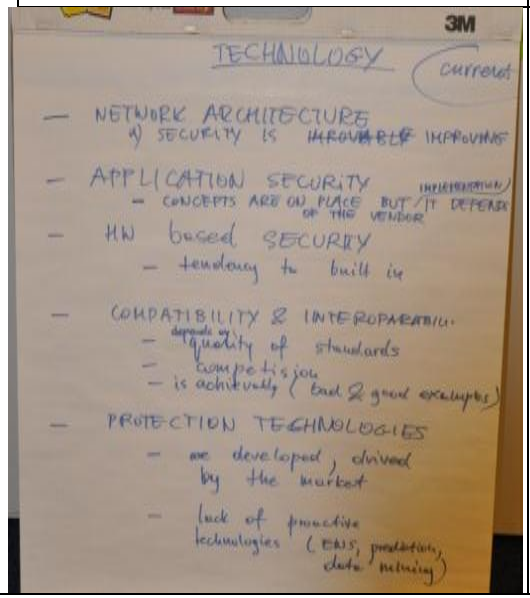
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Technology	• Network architecture (security is improving) • Application security (Concepts are on place but implementation depends of the vendor) • Compatibility and interoperability depends on: quality of standards, competition, is achievable (good & bad examples) • Protection technologies: are developed, driven by the market; lack of proactive technologies (EWS, prediction, data mining)			
				

Table 31: Cyber key factors and future projections - Technology (own compilation)

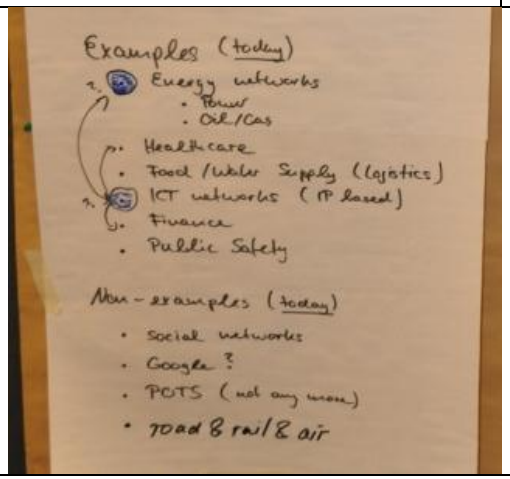
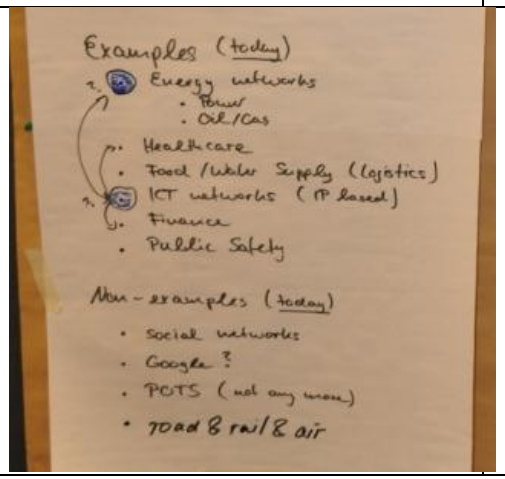
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Critical infra-structure	Examples • Energy network (power, oil/gas) • Health care • Food/Water supply (logistics) • ICT networks (IP based) • Finance • Public safety • Non examples • Social networks • Google? • POTS (not any more) • Road & rail & air	Examples • ICT networks (cloud providers) • ICT applications & services (social networks?, SaaS (->centralization), searching/indexing ->disinformation) • Will quality of SW/Information become critical? • Sensor networks (e.g. GPS, CCTV, …) Non examples • Power? (at last, less than today due to distribution) • Research institutes		
				

Table 32: Cyber key factors and future projections - Critical infrastructure (own compilation)

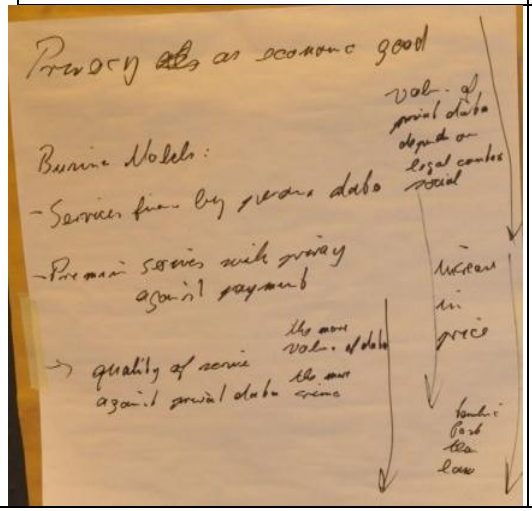
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Privacy	Privacy as an economic good Business Models: • Value of information → change of perception (e.g. mail address) • Accepted business models • Agreement/usage of service • Society not aware of danger/problems	Privacy as concept will disappear, peoples' behaviors become fully transparent • Personal information remains an economic good, but values will drop - >less attractive for attackers • Priority on integrity protection, less on usage control • Market for personalized services will increase brokerage services wider distribution of data -> fine-grained protection domains Examples: travel, car2car, retail		
				

Table 33: Cyber key factors and future projections - Privacy (own compilation)

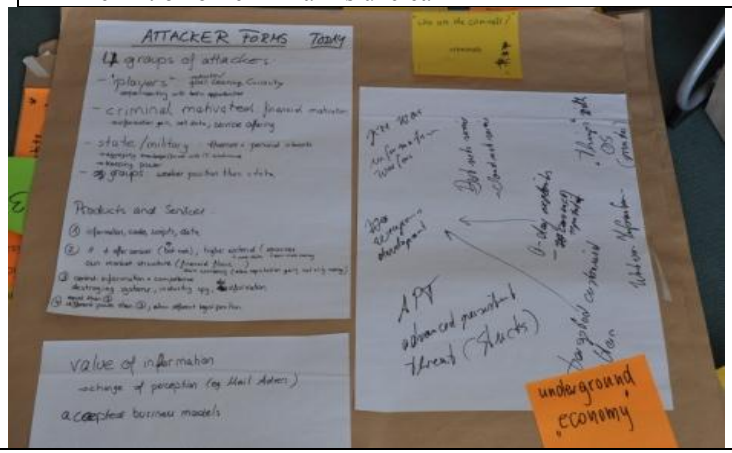
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Attacker forms	4 Groups of Attackers • ‚Players': motivation/goal: learning curiosity, experimenting with technical opportunities • Criminal motivated: financial motivation, -> information gain, sell data, service offering • State/military: themes & personal interests -> aggregating knowledge/force with IT background, keeping power • Groups: weaker position than state Products and Services: • Information, code, scripts, data • Information + offer services (e.g. bot net); higher extend (more data)/resource (earn more money) Own market structure (financial flows,…), own currency (also reputation gain, not only money) • Central: information + competence; destroying systems; industry spy; delete information • Equal than 'Central', different power than 'Central'; also different legal position • Definition of 'criminal' is unclear			
				

Table 34: Cyber key factors and future projections - Attacker forms (own compilation)

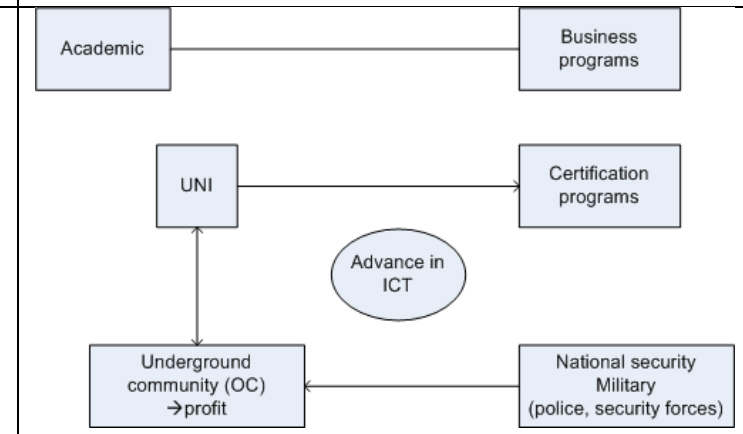
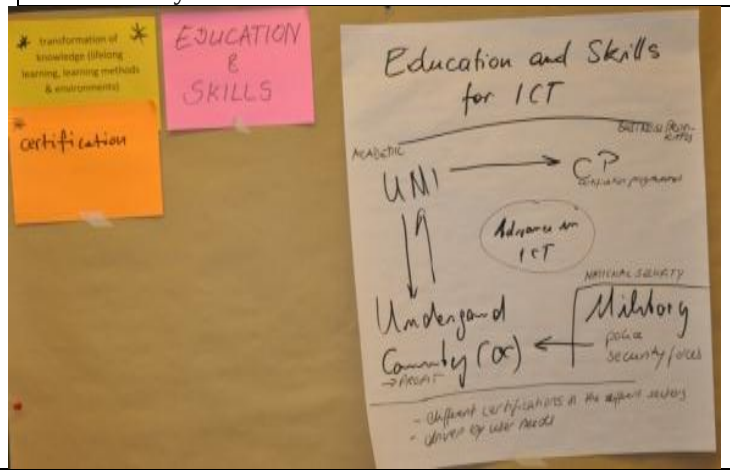
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Education and skills for ICT	 • Different certifications in the different sectors • Driven by user needs 			

Table 35: Cyber key factors and future projections - Education and skills for ICT (own compilation)

2.2 FINDINGS OF THE WORKSHOP ON NUCLEAR

The cluster with aspects relevant for context and the domain nuclear, which build the base for the discussion in focus group workshop overlap and therefore could be useful for linking the context and domain scenarios (see figure 5 below).

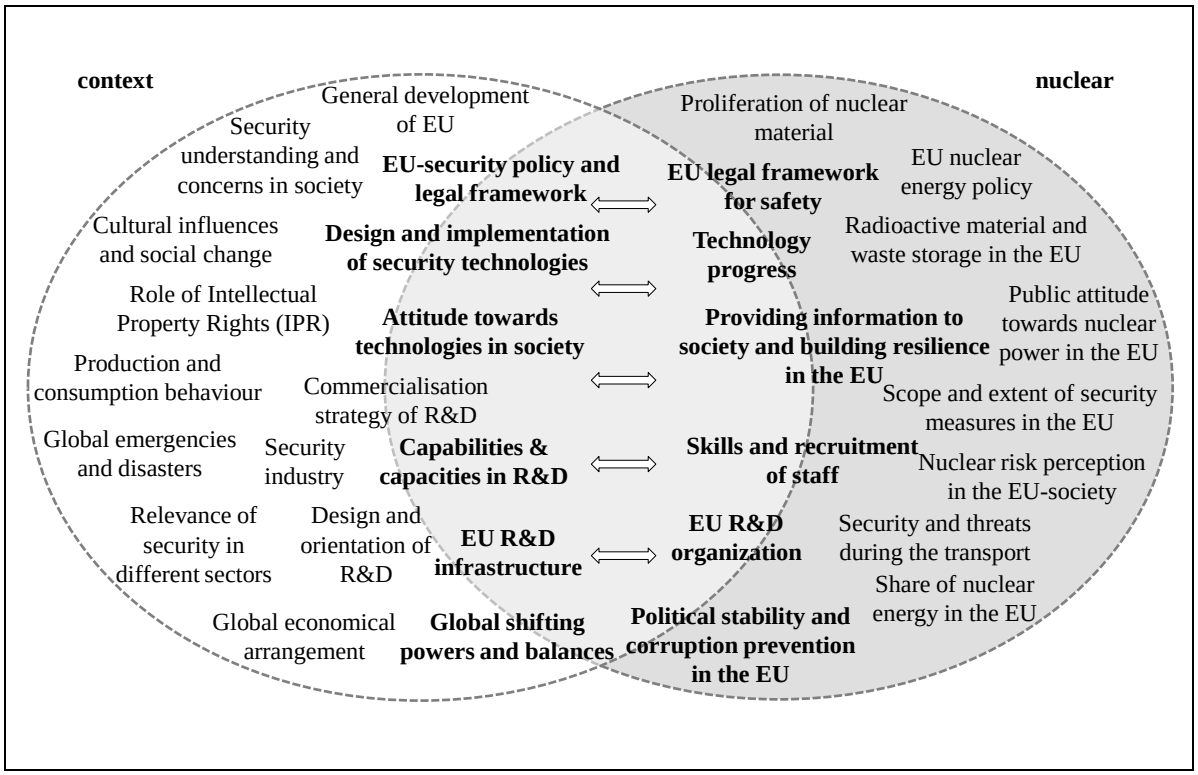


Figure 5: Overlaps between context and nuclear (own illustration)

2.2.1 Context

Based on the contextual aspects presented in the table 2 (see white sheets, tables 35 to 45) the experts discussed and added further relevant aspects (see yellow cards). Subsequent work was to prioritize the most important aspects regarding the following criteria:

- Relevance for the future (time horizon 15-20 years)
- Relevance for the EU
- Relevance for security
- Relevance for the society
- Relevance for the domain nuclear

The following caption applies to tables 35 to 45:

Aspects gained from the key factor stocktaking *Aspects gained from the experts input in workshop* * Prioritized by experts

- *Non-compliance → sanctions*
- institutional development (legitimacy, confidence) ****
- shaping world developments, global foreign policy issues
- *Right to protest (ECHR) (democratic culture)*
- transnational security *
- financial crisis
- regulation & self-regulation
- *"effective" governance and institutions*
- model of responsibility and response
- compliance
- Harmonization ****
- *European energy strategy*
- *Democratic culture* **

Table 36: Factor evaluation for context scenarios - EU-policy and development (own compilation)

- security policy (international, human …)
- *Harmonization* / internationalization of economic policy
- trade embargos, protectionism
- defense (military power, frontier disputes, deterrence, militarization of space)
- fiscal imbalances (public debt, …)
- Incentives
- *Competition, confrontation* *****

Table 37: Factor evaluation for context scenarios - International policy environment (own compilation)

- attitude towards new technologies
- radicalization (shift in political beliefs, social and religious tensions) **
- societal inequality (social tensions, wealth concentration)
- shifting cultural and social influences (e.g. from Americanization to Asian cultural influences)
- sustainable society **
- urbanization vs. rural population
- attitude towards organized crime, corruption & privacy
- traditional and virtual communities (social networks, digital identity, more literate society)
- *Public confidence and support* ****
- *Individual or national ethical or religions issues*
- *Clash of civilizations*
- *Population density*
- *New Media (new information, changing opinion)* *

Table 38: Factor evaluation for context scenarios - Socio-cultural developments (own compilation)

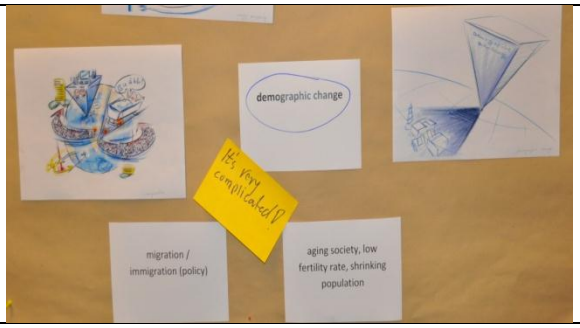
	• aging society, low fertility rate, shrinking population • Migration / immigration (policy) • *It's very complicated!*

Table 39: Factor evaluation for context scenarios - Demographic change (own compilation)

	• technology development (decrease, stagnation, growth) ** • *Break through developments* ** • disruptive technologies • convergence & interoperability • user acceptance **** • interconnection of technologies • user needs ** • *Nuclear (& other weapons) proliferation* • *Market driven profit*

Table 40: Factor evaluation for context scenarios - Trends and drivers in technology (own compilation)

	• balance of institutional participation (e.g. EU, universities, research institutes, enterprises) • commercialization strategy • interdisciplinary & networking • innovation systems (level, actors, institutions, organization) • research governance * • providing information to society **** • bias / focus of research areas

Table 41: Factor evaluation for context scenarios - R&D characteristics (own compilation)

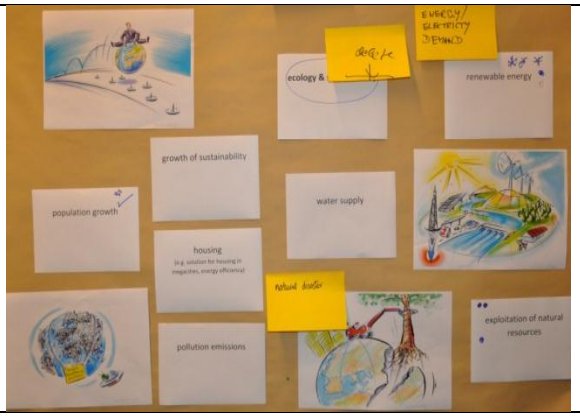
	• growth of sustainability • population growth ** • housing (e.g. solution for housing in megacities, energy efficiency) • renewable energy ***** • exploitation of natural resources *** • water supply • pollution emissions • *Natural disaster* • *Energy/ electricity demand*

Table 42: Factor evaluation for context scenarios - Ecology (own compilation)

	• Terrorism • *What can we do?* • (global) economic situation (recession, crisis, breakdown) ***** • resource scarcity • deterrence (e.g. weapons of mass destruction, arms race) • authoritarian political systems (instability sources, critical systems) • humanitarian emergencies • governance architecture **** • *Compliance and regulation (national an EU wide)* • *Unforeseen impact like 9/11, Fukushima* • *Unforeseen political change like ‚end of cold war'* • *Education of public/citizens (communication)* • *Trust in institutions and the processes* • *Social system*

Table 43: Factor evaluation for context scenarios - Stability, complexity and resilience (own compilation)

	• economic growth (consumption, extent of service sector, manufacturing productivity) • economic policy (competition policies, types of competition) • shifting power and balances (e.g. the Asian Meridian) *** • relations & alliances between politics and business • reversal of economic globalization • economic crime • geopolitics • international cooperations ***** • *Reliability of access to energy resources ** • *Natural resources (geology)* • *Reserved financial funds*

Table 44: Factor evaluation for context scenarios - Economy (own compilation)

	• energy ****** • food * • health * • telecommunication • public administration *

Table 45: Factor evaluation for context scenarios - Relevant sector (own compilation)

	• new production models (work flow etc.) ***** • changing realities in labour markets, virtuality • highly qualified workers • work life balance, business paradigm

Table 46: Factor evaluation for context scenarios - Labour and production models (own compilation)

2.2.2 Nuclear

Based on the contextual aspects presented in the table 4 (see yellow cards, tables 46 to 54) the experts discussed and added further relevant aspects (see orange cards). Subsequent work was to prioritize the most important aspects regarding the following criteria:

- Relevance for the future (time horizon 10-15 years)
- Relevance for the EU
- Relevance for security
- Relevance for the society

The following caption applies to tables 46 to 54:

Aspects gained from the key factor stocktaking *Aspects gained from the experts input in workshop* * Prioritizing by experts **Detailed discussion** (formulating key factors and future projections)

	• quantities of nuclear materials * • number of sites • *If the site is mismanaged, who is to blame? (government or private agency)* • types of nuclear materials **** • energy mix * • frequency of materials transport • materials production / elimination trends • *Access to nuclear raw material* • emergency response capabilities • nuclear infrastructure protection plan ** • nuclear as an economical sector (market structures / development) • **structure of the supporting nuclear industry infrastructure *** • ***Know-how, knowledge preservation (!?skills!?)******* • *Accountability and auditable safeguards*

Table 47: Factor evaluation for domain nuclear - Quantities and infrastructure (own compilation)

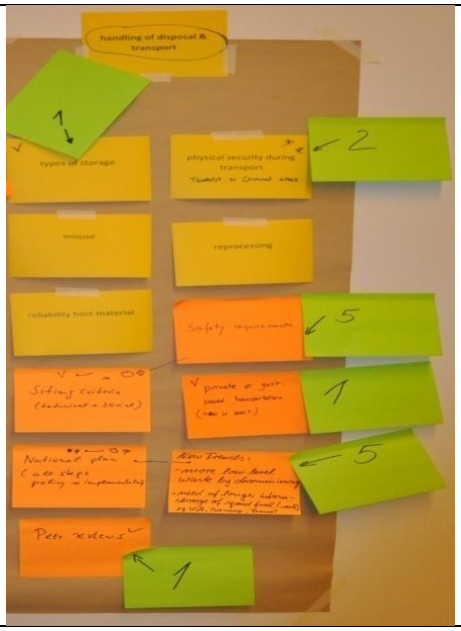
	• physical security during transport ** • *Terrorist or criminal attack* • types of storage * • misuse • reprocessing • reliability host material • ***Safety requirements*** • ***Sitting criteria (technical + social) ******** • *Private or governmental based transportation (who is best?) ** • ***National plan (all steps policy → implementation) ******** • ***New trends*** • ***More low level waste by decommissioning*** • ***Need of longer interim-storage of spent fuel (waste), e.g. USA, Germany, France*** • *Peer Reviews* *

Table 48: Factor evaluation for domain nuclear - Handling of disposal and transport (own compilation)

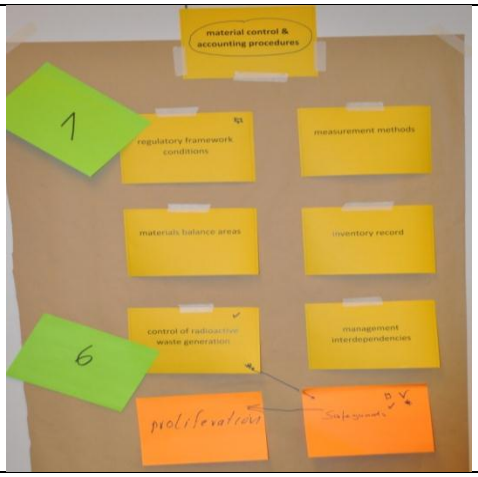
	• regulatory framework conditions * • measurement methods • inventory record • materials balance areas • management interdependencies • control of radioactive waste generation ** • ***Safeguards ******** • ***Proliferation***

Table 49: Factor evaluation for domain nuclear - Material control and accounting procedures (own compilation)

	• criminal prosecution • policy flexibility • regulatory framework (trend / increase / decrease) vs. self regulation **** • harmonization of regulations *** • Taxes • *New programs for nuclear energy (Poland) vs. phaseout (Germany) ** • *Same standards in each of the 27 EU-countries *****

Table 50: Factor evaluation for domain nuclear - EU-policy (own compilation)

	• international legal commitments ** • voluntary commitments • nuclear security and materials transparency • national legal framework ** • *Compliance with international regulations and controls (IAEA)* • *Safety requirements ****** • *Security understanding & perception of protection (?!societal factors!?) ****

Table 51: Factor evaluation for domain nuclear - Global norms and legal framework (own compilation)

	• private/ public/ governmental duty (e.g. PPP) • perception of protection necessity • education/ providing with information * • safeguards adoption & compliance • **institutional setting (independent regulatory agencies) ***** • ***'Joined up' thinking and actions **** • *Emergency plans*

Table 52: Factor evaluation for domain nuclear - Protection responsibility (own compilation)

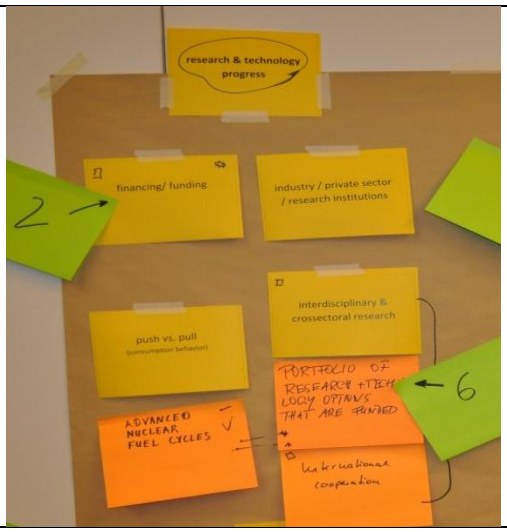
	• industry / private sector / research institutions • financing/ funding ** • push vs. pull (consumption behavior) • **interdisciplinary & cross-sectoral research *** • ***Portfolio of research & technology options that are funded ***** • ***Advanced nuclear fuel cycles ***** • ***International cooperation ****

Table 53: Factor evaluation for domain nuclear - Research and technology progress (own compilation)

	• skills (security personnel vetting, performance demonstration) • *Rich vs. poor* • infrastructure investments * • **certification ***** • **talents & highly qualified (e.g. recruiting processes)** • ***Culture of excellence ***** • ***Attractiveness of jobs in nuclear world*** • ***Older employees / no new employees ***** • ***Management of knowledge ****

Table 54: Factor evaluation for domain nuclear - Human resource factor (own compilation)

	• security understanding & perception of protection • user awareness of threats • **political stability (social unrest, international disputes or tensions, armed conflict) **** • **pervasiveness of corruption **** • groups interested in illicitly acquiring materials • human health issues • adoption of new technology * • *Big society driven* • *Fear of the unknown* • *Change of media (new media)* *** • *acceptance* ***

Table 55: Factor evaluation for domain nuclear - Societal Factors (own compilation)

The focus of the further work was on identifying, prioritising and discussing the key factors and their future projections in small groups (see tables 55-61).

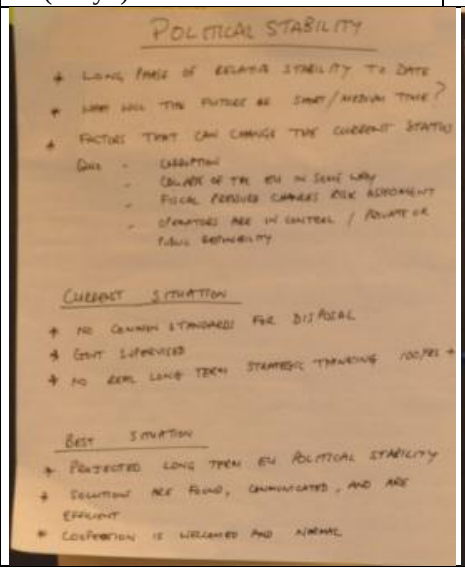
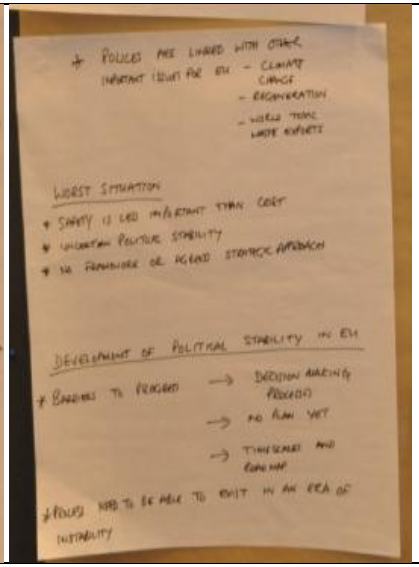
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Political stability / pervasiveness of corruption	• Long phase of political stability to date • What will the future be short/medium time? • Factors that can change the current status quo: corruption; collapse of the EU in some way; fiscal pressure changes risk assessment; operators are in control / private or public responsibility • No common standards for disposal • Government supervised • No real long term strategic thinking (100y+)	Worst Case: • Safety is less important than cost • Uncertain political stability • No framework or agreed strategic approach	Best Case • Projected long term EU political stability • Solutions are found, communicated, and are efficient • Cooperation is welcomed and normal • Policies are linked with other important issues for EU: climate change; regeneration; world toxic waste exports	
				

Table 56: Nuclear key factors and future projections - Political stability and pervasiveness of corruption (own compilation)

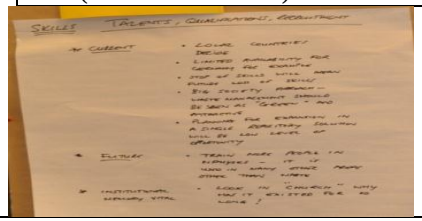
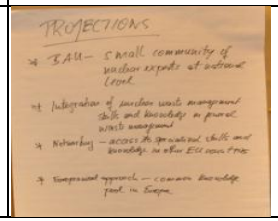
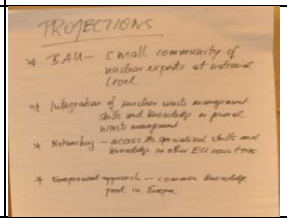
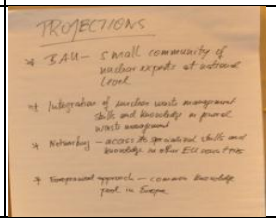
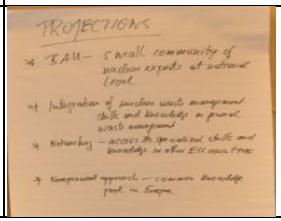
Key factor	Situation today	Future projection A	Future projection B	Future projection C	Future projection D
Skills, talents, qualification and recruitment	• Local countries decide • Limited availability for Germany for example • Stop of skills will mean future loss of skills • Big society approach – waste management should be seen as 'green' and attractive • Planning for expansion in a single repository solution will be low level of opportunity • Future: train more people in nuclear physics – it is used in many other areas than waste • Institutional memory vital: look in "church" – why has it existed for so long? • Public challenge: is healthy and democratic and should be encouraged • Partnership approach: new community will have to be more inclusive to include new levels of new management issues • Open and transparent: common language and communication leading to common understanding • Advantage approach: what are the benefits to communities and operators (direct and indirect)	BAU – small community of nuclear experts at national level	Integration of nuclear waste management skills and knowledge in general waste management	Networking – access to specialized skills and knowledge in other EU countries	Europeanized approach – common knowledge pool in Europe
					

Table 57: Nuclear key factors and future projections - Skills, talents, qualification and recruitment (own compilation)

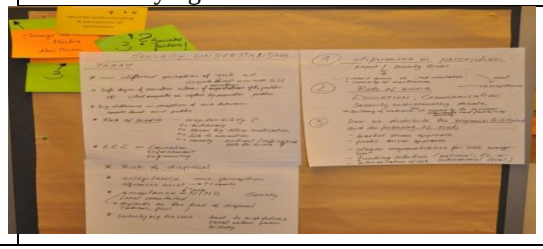
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Security understanding	1. Differences in perception (expert / societal level) - 100% secure vs. „risk-orientation“ - capacity of resilience → direct acceptance 2. Role of media: education, communication - security understanding debate → building of resilience → capacity to recover robustness and flexibility society 3. How we distribute the responsibility(-ies) and the financing of risk - market driven approach - public driven approach - clearer responsibilities for risk management - funding solution (national, EU or international level) - internalization of risk • No different perception of risk at experts level overall EU • High degree of variation in terms of perception of the public or silent majorities vs. capture by minorities problem • Big difference in perception of risk between experts level and public • Role of media: responsibility; autonomy; driven by other motivation; link to education; society: critical / self critical with the media? • Risk of (financial) disposal • Acceptance → perception (differences in acceptance exist between experts and society) • Acceptance → NIMB Society local orientated (acceptance depends on the kind of disposal (interims, final,…) • Underlying reasons: trust to institutions social-culture factor history			
				

Table 58: Nuclear key factors and future projections - Security understanding (own compilation)

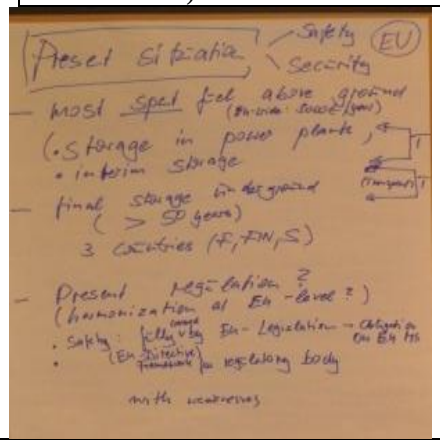
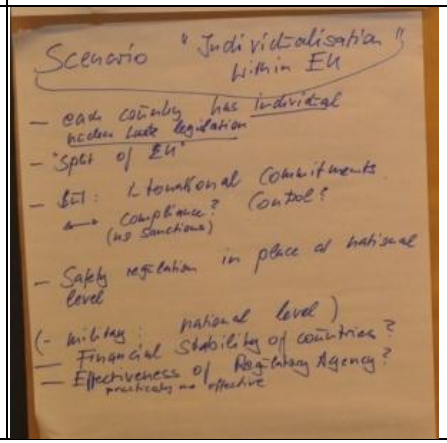
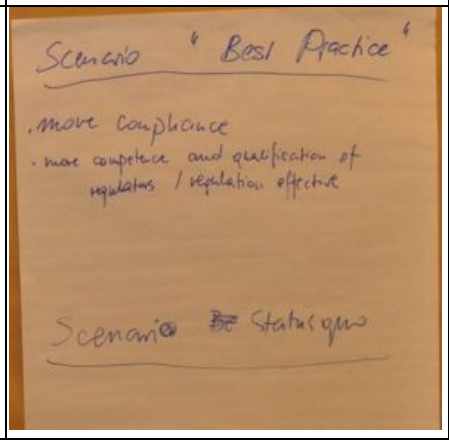
Key factor	Situation today	Future projection A	Future projection B	Future projection C
safety requirements / national legal framework / institutional setting / international legal commitments / compliance with international regulations and controls	• Most spent fuel above ground (EU-wide 3000t/y) (storage in power plants / interim storage) • Final storage underground (>50y), 3 countries (F, Fin, S) • Transport between storage in power plants and interim storage as well as finale storage • Present regulation? (harmonization at EU level?) -safety: fully covered by EU legislation → obligation on EU MS -(EU directive) framework for regulatory body (with weaknesses)	„Individualization within EU“ • Each country has individual nuclear waste legislation • „split of EU“ • Bul: international commitments <-> compliance? (no sanctions), control? • Safety regulation in place at national level • (military: national level) • Financial stability of countries? • Effectiveness of regulatory agency? practically not effective	„Best practice“ • More compliance • More competence and qualifications of regulators / regulation effective	„Status quo“ Nothing changes
				

Table 59: Nuclear key factors and future projections - Safety requirements (own compilation)

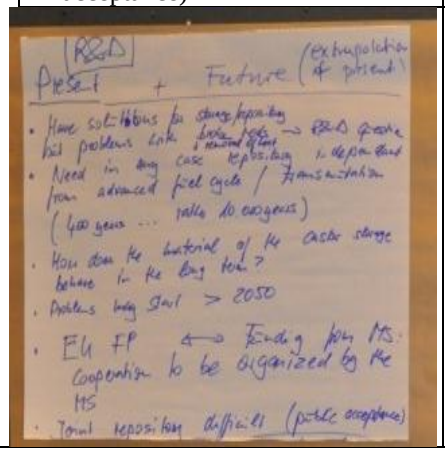
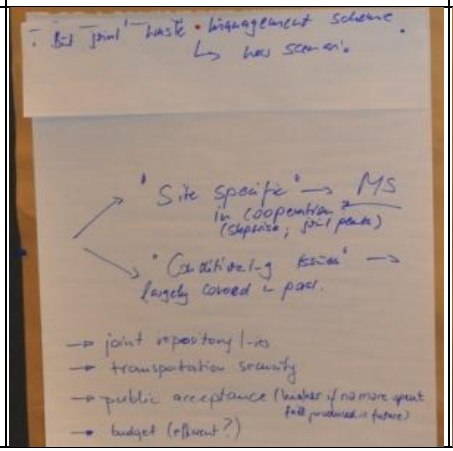
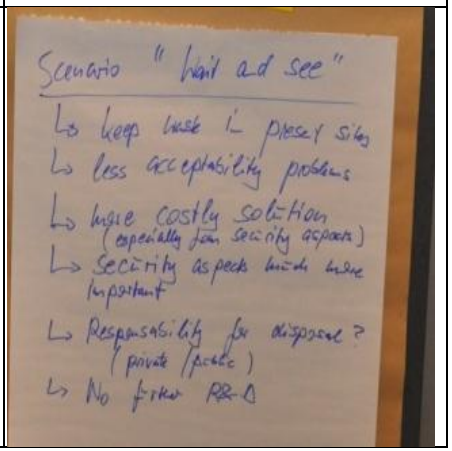
Key factor	Situation today	Future projection A	Future projection B	Future projection C
R&D advanced nuclear fuel cycles / International cooperation	• Have solutions for storage/repository but problems with broken rods + remove of heat → R&D question • Need in any case repository independent from advanced fuel cycle / transmutation (400y … rather 10.000y) • How does the material of the castor storage behave in the long term? • Problems may start >2050 • EU FP <-> funding from MS: cooperation to be organized by the MS • Joint repository difficult (public acceptance)	„Status quo“ Nothing changes	joint waste management scheme • “Site specific“ -> MS (in cooperation?) (stepwise, joint plants) • “Conditioning issues“ -> largely covered in past • joint repository(-ies) • transportations security • public acceptance (higher if no more spent fuel produced in future) • budget (efficient?)	„wait and see“ • Keep waste in present sites • Less acceptability problems • More costly solution (especially from security aspects) • Security aspects much more important • Responsibility for disposal? (private/public) • No further R&D
				

Table 60: Nuclear key factors and future projections - R&D (own compilation)

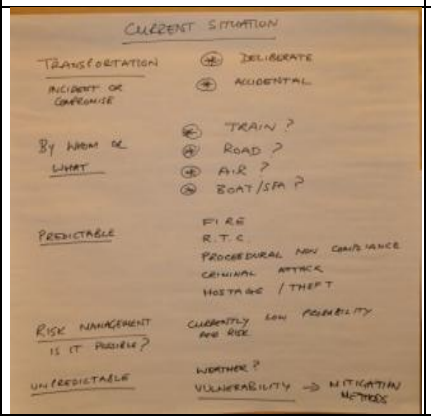
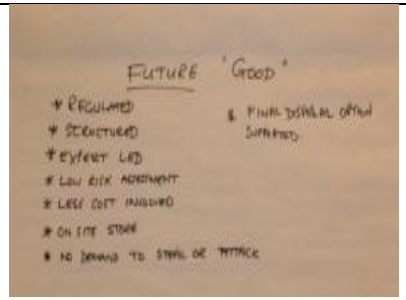
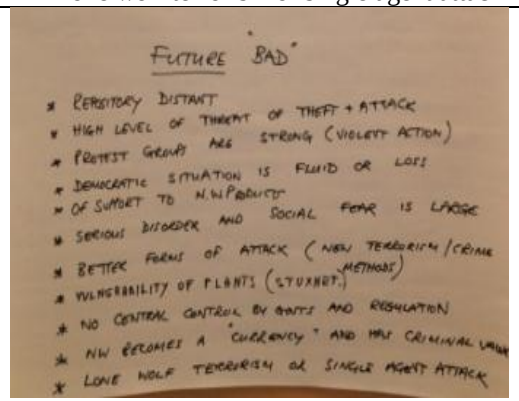
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Physical security during transport	• Transportation (incident or compromise): deliberate; accidental • By whom or what: train; road; air; boat/sea • Predictable: fire; R.T.C.; procedural non compliance; criminal attack; hostage/theft • Risk management (is it possible?): currently low probability and risk • Unpredictable: weather?; vulnerability -> mitigation methods	Good Case • Regulated • Structured • Expert led • Low risk assessment • Less cost involved • On site store • No demand to steal or attack • Final disposal option supported	Bad Case • Repository distant • High level of threat or theft + attack • Protest groups are strong (violent action) • Democratic situation is fluid or loss • Of support to nuclear waste products • Serious disorder and social fear is large • Better forms of attack (new terrorism/crime methods) • Vulnerability of plants (stuxnet…) • No central control by governments and regulation • Nuclear waste becomes a „currency“ and has criminal value • Lone wolf terrorism or single agent attack	
				

Table 61: Nuclear key factors and future projections - Physical security during transport (own compilation)

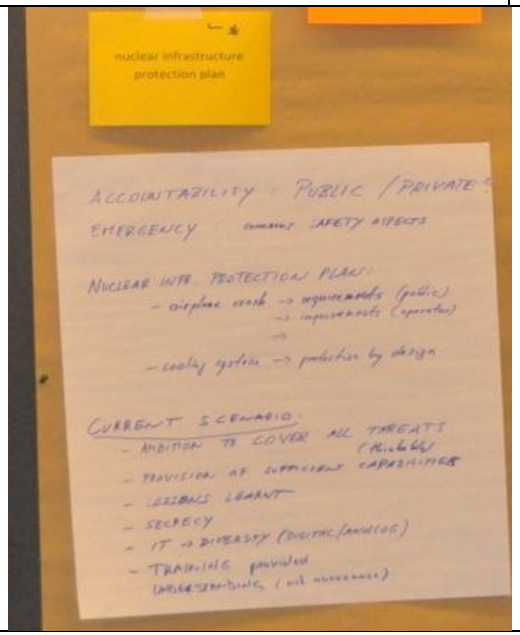
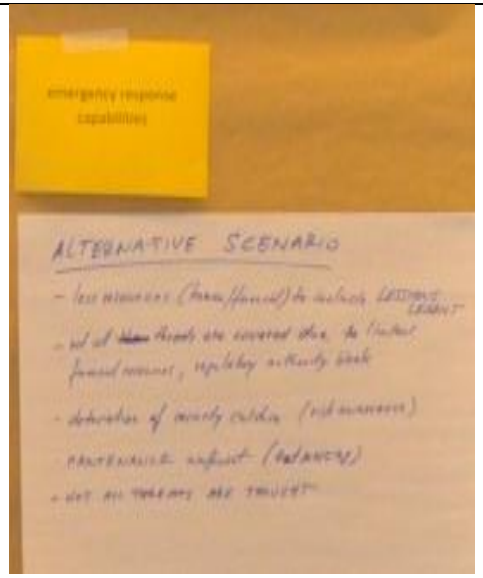
Key factor	Situation today	Future projection A	Future projection B	Future projection C
Accountability (public/private) **Emergency (concerns safety aspects)** **Nuclear infrastructure protection plan**	• Ambition to cover all (thinkable) threats • Provision of sufficient capabilities • Lessons learned • Secrecy • IT→diversity (digital/analog) • Training provided understanding (risk awareness)	• Less resources (human / financial) to include -> lessons learned • Not all threats are covered due to limited financial resources, regulatory authority weak • Deterioration of security culture (risk awareness) • Maintenance insufficient (outsourcing) • Not all threats are thought		
				

Table 62: Nuclear key factors and future projections - Accountability/ Emergency/ Nuclear Infrastructure Protection (own compilation)

3 SUMMARY AND OUTLOOCK OF FURTHER RESEARCH

In the course of the reworking of the workshop results, the sources used for the stocktaking of the key factors will also be used for the identification and description of vague developments of all high prioritised key factors, which were not discussed in the focus group workshops. The description of the key factors (see tables 27-34 and 55-61) will be reformulated by addition of further information to the developed future projections as well as by addition of further projections.

For evaluating the key factors and developing of the future projections in the domain environment another approach is planned:

- Firstly: Interviews with a small number of experts to prioritise the suggested key factors (see table 5).
- Secondly: A survey among at least 20-30 experts to gain information about the possible future developments of the key factors.

Furthermore the key factors and future projections of the high prioritized aspects in the context will be identified and formulated. The future projections of these key factors will build the base for the scenario development. The different future projections, which describe possible developments of the different key factors, will be bundled to alternative scenarios (see the marked line in the table 62 which shows one example of a bundle of future projections). The different bundles of the future projection will be formulated to short scenario stories (1-2 pages) for the context scenarios as well as for the threat scenarios (see an example of a scenario storyline in the figure 6 below). Each scenario should have a high internal consistency and high diversity to other scenarios. For the consistency check between the future projections further workshops are planned, an internal workshop for WP4 members and an internal workshop for all consortium members.

Key factor	Future projection A	Future projection B	Future projection C
The society requirements to the research area	▪ Efficiency and effectiveness is required (evaluation). ▪ Structural change in the national research landscape	status quo Research and education is good per se, the structure of the research landscape and the output of the research is not questioned.	
Exploitation of the research results to increase the economic benefit	In the most relevant social/economic areas an Open Access Strategy is implemented (free access to scientific information).	Even stronger protection: Scientific results are expensive. Patent policies hinder the competition in the commercial exploitation of R&D results.	
Europe's attractiveness as a place to live and work	Europe is even more attractive, by the strengthening of the positive characteristics and a good marketing. English has become the language of science. The labour market is harmonized.	Attractiveness decreases by a lack of marketing and a neglect of the original positive characteristics. Xenophobia is a political instrument.	
Numbers of R&D professionals due tc the demographic changes	National staff resources are not sufficient. ▪ Consequences: international recruitment, the attractiveness for researchers will be strengthened through various measures. The best talent is following the best deals.	The problem of declining numbers of R&D professionals is not being solved. ▪ Consequences: specialisation, relocation of production and research sites to regions outside of Europe	
Economic situation	Global economic recovery ▪ The limited public funding that is available is being invested in transnational European multiplayer structures.	Crisis persists ▪ Fragmentation: some prosperous areas ▪ EU: reduction of the free budget, bound as structural funds	
Influence of cultura differences on R&D cooperation	Nationalization of research Cultural differences are emphasized	Formation of interfaces Gradual rapprochement of cultures	
Regional bonds of the companies	Status quo	▪ More competences and competition between regions ▪ Hot spots in certain disciplines ▪ There will be a regional shift	
The acceptance of t new technologies o the society and the reaction of the R&D	The acceptance of new technologies in the German society falls: ▪ Ease of use, "simple products" ▪ Rational assessment Handling by R&D: ▪ System integration (e.g. ambient intelligence, integration of multiple devices or functions in one unit) ▪ Privacy plays a major role, data security ▪ Admission requirements increase	Technology Hype: ▪ technology as the solution of sustainability problems (global challenges) ▪ The number of Start-ups increases ▪ Increasing R&D and coordinated global networks	
Societal and politica development of the EU	Strong Development of Europe: ▪ The Treaty of Lisbon has positive effects ▪ There is an European consensus on security and CO2 reduction ▪ Integrated business and work space ▪ People feel connected with Europe.	Europe of different regions (average development): ▪ Europe of different regions with the appropriate constitution, etc. ▪ provision of services in the regions; national level rather unimportant	Return to the interests of their own nation and region: ▪ The EU is no longer capable of making decisions. ▪ The EU as a monetary union is threatened by the bankruptcy of several member states ▪ Cooperation (economic policy, foreign policy) is difficult.

Table 63: An example of a bundle of future projections as a base for one scenario; Source: Behlau et al. 2010

The European puzzle: muddling through

As public resources decrease, competition for research funding increases, at both national and European level. No incentive exists for implementing structural changes or developing a stronger profile in the research landscape. The landscape is determined by large R&D structures, which are historically rooted and mostly uncoordinated. Coordinated action only takes place on a short-term, project-related basis. Owing to the fragmented nature of the European research landscape, its attractiveness for scientists from other regions of the world declines.

The world has largely recovered from the acute economic crisis, but no new structures have been created in the financial sector, and industry is still geared to unlimited growth. These systematic weaknesses impede development of the European Union. The process of integration stagnates and each member country attempts to optimize its own position in the global network in the short term. Without substantial reforms, Europe is stuck in its same old ways.

Figure 6: An example of a scenario storyline; Source: Behlau et al. 2010

All in all to finalize the development of the context based threat scenarios further steps are needed (see underlying points in the figure 6 below):

- Development of context based threat scenarios based on the findings of the focus group workshop: Further research based deriving of the key factors and their future projections to rework the findings from the focus groups and the survey as well as linking the context and domain scenarios using consistency analysis. The challenge will be to handle the different time horizons for context and threat scenarios in the domain cyber infrastructure.
- Identifying threats additional to the threat scenarios: Besides the focus group workshops there are four sources for the identification of threats as well as societal needs, firstly interviews in task 4.1, data mining in task 4.2 and wild cards analysis in task 4.4.
- Scenario validation workshop with end-users and stakeholders as well as project partners for discussing the scenarios and deriving societal needs.

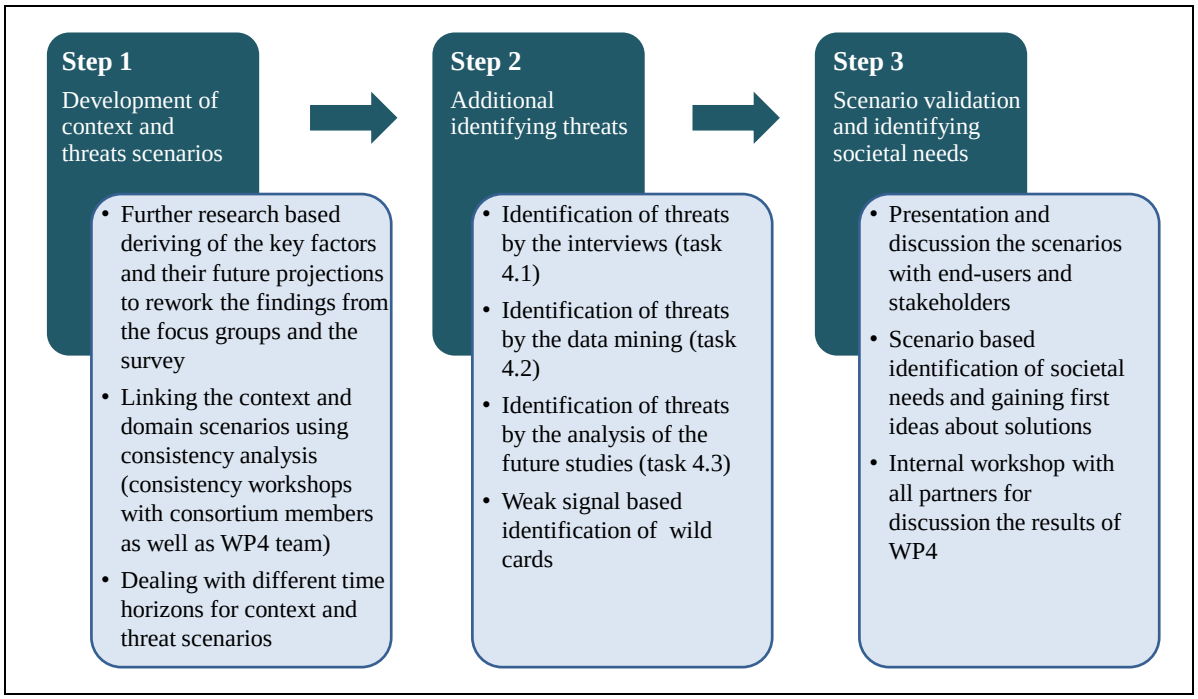


Figure 7: 3-step-proces for development of the context based threat scenarios, (own illustration)

4 APPENDIX

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

4.1 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; Kulas, Andrea; Dönitz, Ewa; Schirrmeister, Elna: *Envisioning future research horizons. Scenarios for the European research landscape 2025*. München: Fraunhofer-Gesellschaft 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, Jennifer Cassingena-Harper, " *SESTI working paper - Major trends, challenges and emerging issues in Health",* European Commissi*on,* 2010

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

Endregard, Monica, Hanne Breivik, 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, 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, Simone Kimpeler, "Wie nutzen wir Informations- und Kommunikationstechnologien im Jahr 2020?", FAZIT-Schriftenreihe, Forschungsbericht / Band 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, 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 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, 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

4.2 CYBER

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

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

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 2011

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

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

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

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

Hange, Michael, " *Schutz und Sicherheit kritischer Informations und Kommunikations-Infrastrukturen", Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2*010

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

Krüger, Kristin, *IT-Sicherheit in der öffentlichen Wahrnehmung*. Magdeburger Journal zur Sicherheitsforschung, Band 1, S. 153–167, 2012

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

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, Prof. Dr. August-Wilhelm Scheer," *Promotorenbericht zum Zukunftsprojekt Sichere Identitäten*", Promotorengruppe Sicherheit

der Forschungsunion Wirtschaft-Wissenschaft, 2012

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

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, Band 2,S. 102–114, 2011

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

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

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

4.3 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”, http://www.ansto.gov.au/__data/assets/pdf_file/0020/46172/Management_of_Radioactive_Waste_in_Australia_v2.pdf, 2011

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

Baisden, Patricia, Gregory Choppin, “*Nuclear Waste Management and the Nuclear Fuel*

Cycle", Encyclopedia of Life Support Systems, 2007

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

Botella, T., J. Coadou, 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

Burns, W., A. Hughes, J. Marples, R. Nelson, 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, http://www.nap.edu/catalog/11263.html, 2006

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

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

Deutch, John M., Dr. Charles W. Forsberg, Prof. Andrew C. Kadak, Prof. Mujid S. Kazimi, Prof. Ernest J. Moniz, 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, 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

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

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, 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, 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

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

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

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

IAEA, "Developing multinational radioactive waste repositories: Infrastructural framework and scenarios of cooperation", Austria, 2004

IAEA, "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

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

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

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

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

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

Lidskog, Rolf, 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

Matzke, Hj.,"*Radiation Damage Effects in Nuclear Materials*", Nuclear Instruments and

Methods in Physics Research, 1988

Murray, James, Joseph Harrington, 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

Neumann, Wolfgang,"*Nuclear Waste Management in the European Union: Growing Volumes and No Solution*", INTAC, 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", http://www.nei.org/resourcesandstats/Documentlibrary/Nuclear-Waste-Disposal/whitepaper/reprocessingandrecycling, 2006

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

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

Price Stephane and Lynn, "*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, 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

Taylor, 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

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

Wikipedia, “Waste management in Bangladesh”, http://en.wikipedia.org/wiki/Waste_management_in_Bangladesh, 2013

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

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

4.4 ENVIRONMENT

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

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”, http://www.livediverse.eu, 2010

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 17(2): 10., 2012. http://dx.doi.org/10.5751/ES-04794-170210

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

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

Druel, E., Billé, R.,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 Directorate-General for Environment, “Study on understanding the causes of biodiversity loss and the policy assessment framework”, 2009

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

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

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

Herold, M., Couclelis, H., 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., Wesman, C. A., "Roles of scale, matrix, and native habitat in supporting a diverse suburban pollinator assemblage", Ecological Applications, 22(7), pp. 1923–1935, 2012

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

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

Intergovernmental Panel on Climate Change (IPCC), *"IPCC Special Report Emissions Scenarios," ISBN: 92-9169-113-5,* 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

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

King, David, "Foresight Future Flooding, *Chapter 7 Environmental impacts of future flood risk" Foresight Directorate DTI, 1, Victoria Street London SW1H 0ET, http://www.foresight.gov.uk*

Lambin, Eric F. et al., "The causes of land-use and land-cover change: moving beyond the

myths“, Elsevier Science Ltd, 2000

Leemans, Rik, “Applying global Change Scenarios to Assess Changers in Biodiversity”, Bilthoven, 1999

Litvinovitch, Jutta, Björn Ingendahl,“ *Klimawandel, Extremwetterereignisse und Gesundheit*“, Konferenzbericht, Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU), 2010

Meijl, H. van, T. van Rheenen, A. Tabeau, 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) und 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, F. Jiguet, “Different policy scenarios to promote various targets of biodiversity”, http://www.elsevier.com/locate/ecolind, 2011

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

OECD, “*OECD Environmental Outlook to 2050*, “ OECD Publishing 2012

OECD, “OECD Environmental Outlook to 2050”, OECD Publishing, http://dx.doi.org/10.1787/9789264122246-en, 2012

OECD, “*Towards Green Growth*“, OECD Publishig, 2011, http://www.oecd.org/dataoecd/42/39/48432900.pdf

OECD, H“*OECD-FAO Agricultural Outlook 2012-2021*“, OECD Publising 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“, American Association for the Advancement of Science, Science 330, 2010

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, www.sciencemag.org, VOl287, 2000

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

Sala, Osvaldo E.,“Consequences of changing biodiversity”, Macmillan Magazines Ltd, Macmillan Magazines Ltd,ol 405, 2000

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

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

Spangenberg, Joachim H., “Scenarios for investigating risks to biodiversity“, Global Ecology and Biogeography, (Global Ecol. Biogeogr.) 21, 5–18, 2012

The Royal Society, “Measuring biodiversity for conservation”, London, 2003

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

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, “Global Environment Outlook 4“,2007

United Nations Environment Programme, “Securing Sustainability Through the Conservation and Use of Agricultural Biodiversity”, UNEP Division for the Global Environment Facility, 2010

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