D4.2 ETTIS Methodology Note

Deliverable submitted in February 2014 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:	**ETTIS Methodology Note**
Due date:	**31 October 2013**
Actual submission date:	**18 February 2014**
Lead contractor for this deliverable:	**AIT Austrian Institute of Technology GmbH**
Contact:	**Joachim Klerx** joachim.klerx@ait.ac.at
Dissemination Level:	**PU**

Authors:
Joachim Klerx, Austrian Institute of Technology
Ewa Dönitz, Fraunhofer ISI
Sonja Grigoleit, Fraunhofer INT
Henrik Carlsen, FOI, Swedish Defence Research Agency

CONTENT

FIGURES

TABLES

EXECUTIVE SUMMARY

The main objective of this report is to summarize the methodical experience from the research in WP4. In addition, the report takes the opportunity to increase the usefulness of D4.2 for the project as a whole, by taking up some comments on integration of WP4 results into other ETTIS WPs and revises some of the methodical comments from D 3.1. In particular, D4.2 offers the opportunity to make a step towards codification of the envisaged ETTIS methodology, developed against the background of the experiences made in ETTIS to support research agenda setting in the security domain.

The report explains how threats and needs were identified in WP 4 and how scenarios were created out of this. As a main contribution to the methodical discussion in ETTIS, this report refers to the ongoing discussion on how to proceed in WP 5 and WP 6, given the experience from the research in WP4 and WP3.

Scenarios were foreseen to play a key role throughout the whole project. The experience from the work in WP4 confirmed that scenarios are a key methodological constituent of the ETTIS methodology for research and innovation prioritisation. However, a remarkable amount of different types of scenarios were created up to now. In order to integrate the working and findings from WP4, WP5 and WP6, it is crucial to have the right level of abstraction in these different types of scenarios. Up to now, we have created broad context scenarios, more specific threat scenarios, and detailed challenge scenarios in ETTIS. The definitions of these different types of scenarios are presented in the glossary of this report, but the purpose and meaning for ETTIS, as well as relationships between these different types of scenarios needs further elaboration to be clarified. This report has identified some possible development path to combine consistency and diversity analysis for scenario development. Such methodical development is currently taking place in WP5.

This report has laid the ground for the work of identifying and assessing solutions to societal security needs, i.e. the work of WP5. The work in WP4 has been on methodology and content, with the delivery of a huge amount of substantive information. In order to advance the further methodological development in ETTIS, WP5 will show a different balance and focus more on methodical development. However for WP6 a usable list of priorised research topics is necessary. It is an ongoing matter of discussion on which method can be used, to produce this.

WP 6 finally should contribute to the public discussion about future research topics. It is a crucial factor of success to streamline the results from WP 4 and WP 5 to feed into the methodical concept of WP6. Therefore, all methodical insights are discussed and assessed against the background of the main goals of ETTIS.

1 INTRODUCTION

By discussing and addressing the methodical issues that we encountered in WP4 and putting forward some initial methodical ideas to be used in WP5 and WP6, this report provides some useful insights into the methodical experience of WP4 and the methodological interfaces to WP2, WP3, WP5 and WP6.

This report references to other WP results in ETTIS and tries to give inputs to a meta-discussion on different methods used in ETTIS. In chapter 2 the methodical framework from WP3 is discussed in the light of WP4's findings and changes to this framework are developed. A starting point for the methodical discussion is the position of WP4 in the methodical framework of WP3.

The next three chapter of this report are about the key methodical insights emerging from WP4. WP4 aims to identify threats and needs, and to derive scenarios from them. However, with respect to the timing of the different tasks, this was not a linear process. Initially we had planned to develop scenarios and do the threat identification in parallel. In doing this, we have learned, that instead a better approach was to first identify threats using a combination of document analysis, interviews and IT based weak signal scanning, then to develop scenarios in workshops, and finally identify needs by means of discussions in focus groups. This is reflected in the order of the chapter in this report. Chapter 3 focuses on the threat identification methods. In chapter 4 the scenario methods are discussed and in chapter 5 the methods for need identification are presented.

As scenario methods are used in WP5, chapter 6 deals with the developments of perspectives and options for this, based on WP4 experience.

In chapter 7 the overall experience of WP 4 is reflected upon, in view of the end user and stake holder's interests. Finally n chapter 8 summarises the consequences of WP 4 experiences for the second half of the ETTIS project.

2 THE RESEARCH PROCESS IN ETTIS AND THE POSITIONING OF WP4

In this report, the methodical experience of WP4 is discussed in light of the main goals of the ETTIS project and the interests of the end user and other stakeholder groups in ETTIS.

As mentioned in the ETTIS B-Form, the aims of the ETTIS project are

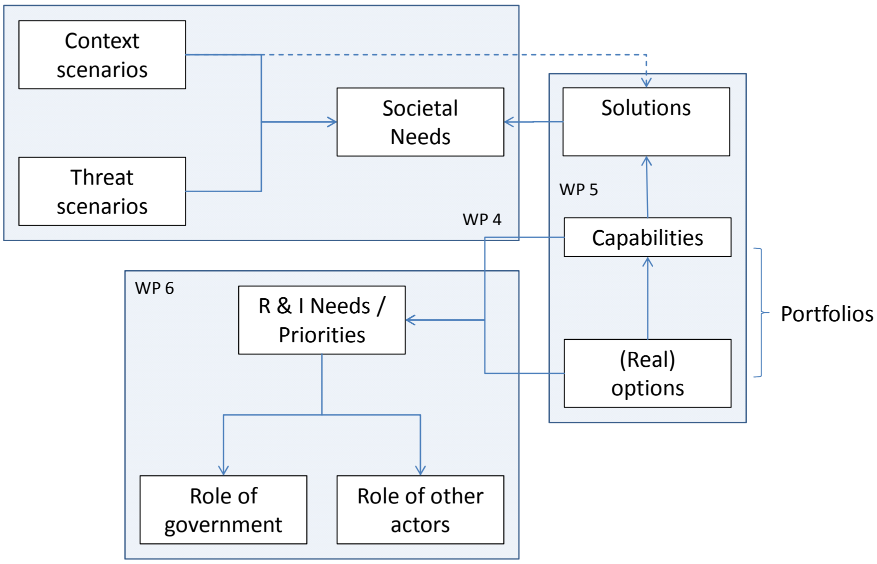
1. *"to identify, understand and assess in a scenarios framework future threats, needs and opportunities for societal security,*
2. *to develop and test a methodological approach and model for a revolving process of security research priority setting,*
3. *to derive research priorities geared towards the needs of user organisations, as well as rationales and options for policy intervention, and*
4. *to help increase awareness of and attention to security research results, and contribute to overcoming barriers by advancing and testing a range of intelligence tools and techniques."*[1]

[1] ETTIS B-Form

In D3.1 a first methodical framework was proposed as a description of the core research process in ETTIS and key activities in WP 4-6 were identified to meet ETTIS' key objectives. After finishing WP 4, this report takes the opportunity to reformulate the research process of ETTIS, based on the experience gained in WP 4. As in every research process, the knowledge about the research process increases in doing the process. In principle, the interdependency of the WPs 4-6 has not changed. However, the research process in WP 4 has lead to a deeper thematic understanding and a more precise language, so that key technical definitions, used in ETTIS, such as threats, scenarios, needs, solutions, capabilities, options and other technical terms have more clearly redefined in this report.

The following figure, developed in D3.1, visualises the research concept, prior to the experience in WP4.

Figure 1: ETTIS core research processes, prior to WP4 research



Source: ETTIS deliverable D3.1

The figure makes clear, that WP 4 serves as input to WP 5 and results from WP5 feed into WP 6. The core idea was that WP 4 produces context scenarios and threats and derives social needs from scenario analysis. It was expected, that the developed scenarios would be at a level of abstraction that would allow the immediate use of the scenarios in the subsequent work packages, in particular WP 5. Furthermore, it was expected, that new knowledge would be created in WP 4 about different types of threats. In addition, the definitions of threats needs and scenarios in the glossary, produced in WP3, have been improved by bringing in the experience from WP 4.

In general, the main objectives from WP4 were originally defined as:

- to identify and anticipate associated future user and societal needs,
- develop context-based threat scenarios,
- and identify key threats to society for further analysis.

These objectives were addressed in the research activities, but it turned out that the topics discovered in WP 4 could not be unequivocally be categorized as threats or needs or options. In fact, it turned out that a primary threat topic can be an option. Furthermore, some threats directly imply certain social needs, whereas other do not. A main result from working with threats was that threats are always related to a subjective interpretation of a specific event. If this event is harmful to someone, or to a group, this group will consider this event as a threat. Conversely, if this event has positive effects for a different group or individuals, they will consider this event as an option or an opportunity.

In doing the research in WP 4 it became clear that methods for threat identification delivered threats, but although needs, capabilities, options, trends, wild cards and other topic classes. In particular, the weak signal scan delivered hints to present and future capabilities, options and solutions. However, the identification of these different categories of topics is only possible by human judgement. Often, this judgement is based on expert knowledge. An unexpected result from WP4 was that it is very difficult to differentiate among threats, needs, opportunities, capabilities, trends, disruptive events and wild cards, even if you have in-depth experience. In addition different methods of threat identification showed different results. But this will be discussed in detail discussed in the threat identification chapter, in detail.

The core research activity in WP 4 focused on the scenario development via workshops, supported by results from other research activities such as threat identification, information mining, interviews and focus groups. The scenarios were then validated by experts in a validation workshop.

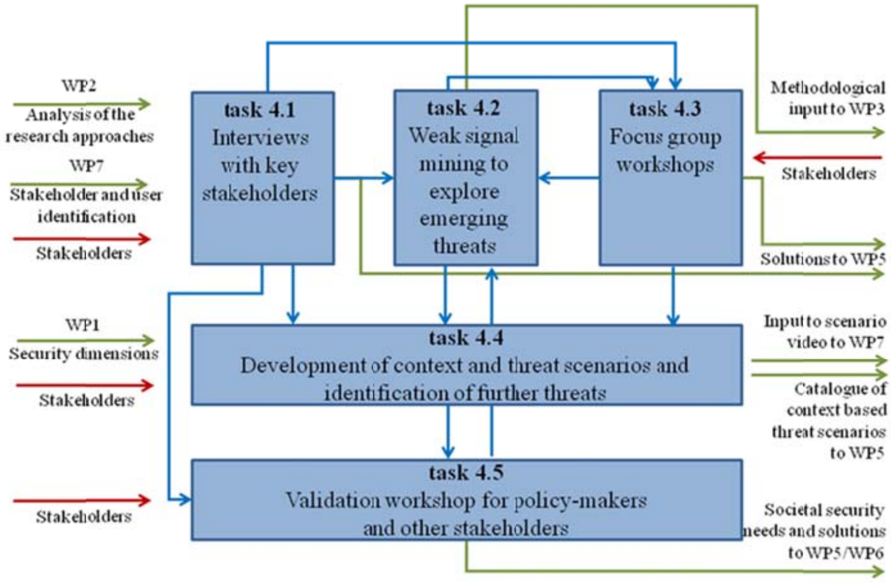
As described in D 4.1, scenario development in WP 4 basically proceeded in two steps: In the first step, **context scenarios** were created. In a second step **threat scenarios** were developed and embedded in the context scenarios. These embedded threat scenarios are called “context based threat scenarios”. (A detailed definition can be found in the glossary of this report.)

Since the beginning of ETTIS there has been an intensive discussion about whether to focus on domains or to work with "the most important threats" of the future. There are advantages and disadvantages of both options. On the one hand, it is a main intention of ETTIS to identify future threats, without any prejudice. On the other hand, most of the methods for threat identification rely on expert judgment, which implies domain knowledge. Choosing experts is only possible within a given domain of expertise. In WP 4, we used a domain-neutral approach whenever possible e (i.e., internet scan) and we defined domains when required (i.e., interviews, focus groups and validation workshop). It was an interesting result that both research directions ended up with the same specification of domains.

The findings from the internet scan pointed to different clusters of threats: cyber security, nuclear security, climate change, ocean acidification, rainforest destruction, different types of anthropogenic pollution (water, air, light, noise, space), genetic threats, invasive species, biomimetic robots and food security. Except for cyber - and nuclear threats, most of the other threats can be clustered as environmental threats. However, in terms of number of sites, the environmental cluster is about 10 times as large, as each of the other cluster (cyber and nuclear). At the beginning of ETTIS, it was suggested by the EC to focus on cyber, nuclear and environment. These three domains were discussed by and confirmed within the consortium. At the beginning of WP4 it was clear, that some methods are in need to specify a specific topic (e.g. focus groups), whereas other methods are not (e.g. internet scanning). With regard to the domain-depended methods, the consortium decided to focus on cyber infrastructure, nuclear and environment as main expert domains. However, the internet scan was done, without any domain filter. After doing this, the clustering results of the internet scan pointed to the direction, that indeed, the predefined domains are also visible in the results of the domain neutral independent scanning.

The results of tasks 4.1 "Interviews with key stakeholders", task 4.2 "Information mining using advanced IT tools to explore potential threats" and task 4.3 "Focus groups" were used to prepare the specific scenarios in each domain. This was the main focus of task 4.4. Subsequently, the scenarios were validated in task 4.5. The following figure, originally presented in D 4.1 provides an overview about the research process in WP 4 and the internal and external interfaces with other WPs.

Figure 2 - Research process in WP 4, with the interfaces per task


WP2
Analysis of the research approaches
WP7
Stakeholder and user identification
Stakeholders
WP1
Security dimensions
Stakeholders
Stakeholders
task 4.1
Interviews with key stakeholders
task 4.2
Weak signal mining to explore emerging threats
task 4.3
Focus group workshops
task 4.4
Development of context and threat scenarios and identification of further threats
task 4.5
Validation workshop for policy-makers and other stakeholders
Methodological input to WP3
Stakeholders
Solutions to WP5
Input to scenario video to WP7
Catalogue of context based threat scenarios to WP5
Societal security needs and solutions to WP5/WP6

Source: ETTIS deliverable D4.1

The **interviews with key stakeholders** provided us with input regarding current and future threats and societal needs. These stakeholders are conventional security research end-users (police, technical relief teams, ministries of the interior, etc.) as well as representatives from public and civil society organisations engaged in societal needs on a general level (religious communities, NGOs, etc.).

The interviews were conducted in two phases. In phase 1 the focus was on the identification of threats and needs and mainly conducting interviews with conventional security research end-user. The aim of the first phase of interviews was to provide the focus group workshops with inputs for the identification of key factors and for the setting of the thematic focus within the three domains (cyber infrastructure, nuclear material and environment).

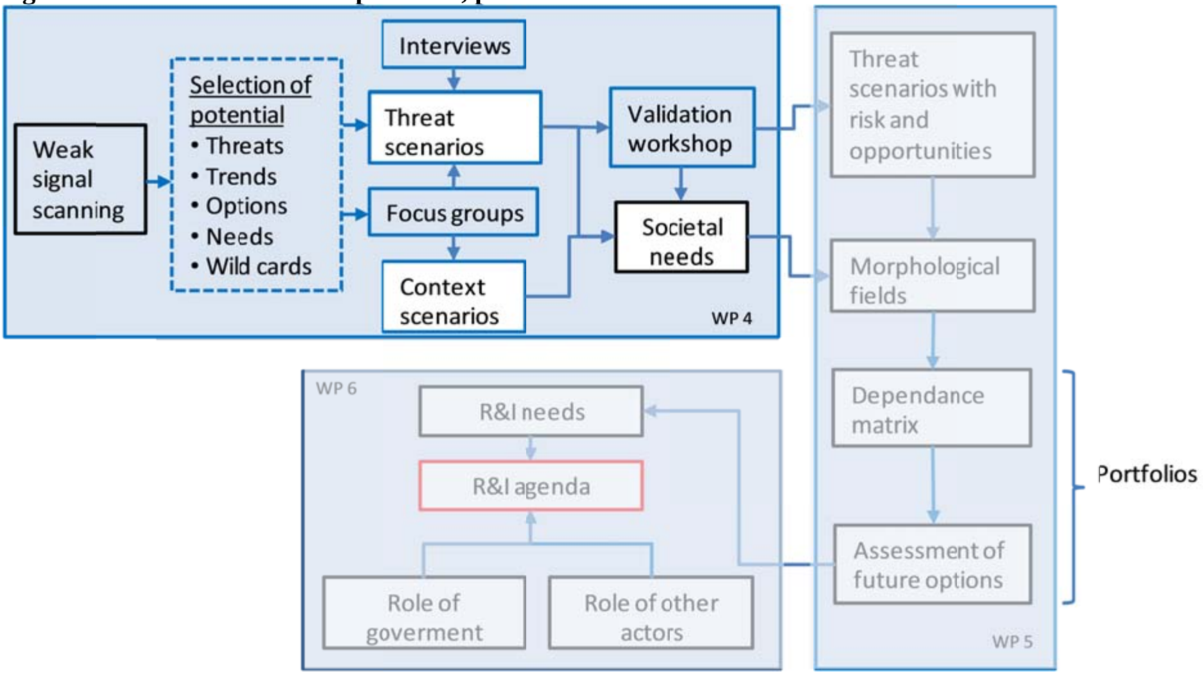
The second phase of interviews took place after the focus group workshops when the first scenario drafts were finished. In the second phase we discussed the needs and security solutions with stakeholders. For the second phase we engaged interview representatives from public and civil society organisations in the development of possible future societal needs.

IT-based weak signal scanning was used to explore emerging threats and societal needs based on sources from internet. The weak signal scanning did deliver all sorts of information about weak signals, trends, options, capabilities, needs, wild cards and other, within the domains and across the domains. In that way it was helpful in specifying the thematic focus within the domains. However, the results needed to be interpreted by human experts since the computer generated classifications did not always make sense. .

The **focus groups** delivered input to the threat identification, trends and needs. This was used to develop scenarios as well as to get a deeper understanding of the contexts of the scenarios. The focus groups did contribute to an analysis to identify and structure all factors influencing the development in present and future time.

Based on the experience from WP 4, the ETTIS core research processes can be visualised more in details as below. The following figure presents the schema of the actual output of WP4 and proposes procedural improvements for future research.

Figure 3: ETTIS core research processes, posterior to WP4 research



Source: ETTIS deliverable D4.2

In the timing of WP4, the weak signal scan and the scenario development were conducted as parallel tasks. However, for future research it would be better to have first the weak signal scan, than, based on the results, the interviews. Both results then should support the discussion in the focus groups. And then by integrating all the findings from all these activities the results the scenarios can be created.

There was a second timing issue in the WP 4 research process. As the scenarios will be used later in the project, specifically in WP5 and WP6, it became apparent that the right level of abstraction needed to be identified, when setting up the scenarios. Having this in mind, the WP 5 and WP 6 teams should have been involved in the scenario building process in WP4, which was not foreseen in the work schedule. In addition WP 5 and WP6 teams should now closely coordinate the further processing of the developed scenarios by keeping in mind that the level of abstraction is important for the usefulness of the scenarios. An abstract scenario might fit to almost every future situation (e.g. a positive developing EU), but is useless for research planning. A specific scenario (e.g. cyber bulling is increasing) does imply a single research option, e.g. do research against cyber bulling and thus is not helpful for research planning.

3 METHODS FOR IDENTIFICATION OF FUTURE THREATS

In this chapter the different methods of threat identification are discussed and advantages and disadvantages of the different methods identified, including a critical review of the quality and usefulness of results.

In general to identify future threats has quite some epistemic challenges. A major problem of threat identification is that the definition of a threat is not clear. In a common sense, a threat results from intentional human activities and is potentially harmful to the security of an individual or a group of humans.

However in the analytical work of WP 4, it became clear, that a threat is a subjective interpretation of a specific event. If this event is harmful to a person or a group, this event is considered as a threat from all group members. This opinion is not necessary shared by other groups or other humans. In particular, there might be another group, who takes advantage from this event. As a result the group usually will not consider this event as a threat. Therefore, threats are always subjective expression of a value. Threats can be a warning that one is going to hurt or punish someone, they can be a sign of something dangerous or unpleasant which may be, or is, about to happen, or they can be a source of danger.[2] In each of those meanings, the following 3 essential elements are part of a threat:

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

This means, that scanning for threats will bring all three components: events, causes and effects. To identify these different elements of a threat we will need then to employ human interpretation.

It is even more difficult to identify future threats, which are not apparent in the present. By definition, some of the future threats are unknown right now, which makes them undiscoverable. However humans have a long tradition in identification of potential harmful events. Therefore, most of the natural harmful events and lots of the manmade harmful events are known. Nevertheless, when it comes to new technological developments and new trends, such as climate change and human waste, we discovered fairly new harmful events.

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

The overall method mix for threat identification deployed in WP 4 is a combination of threat identification from different sources, like:

- Expert knowledge (Interviews)
- Internet (Weak signal mining for future threats)
- and expert literature (future studies)

and interpretation of the results. The interpretation was based on two different methods: :

- Literature research
- and expert workshops

The following chapter 3.1 and 3.2 will give some details about the experience with each method in threat identification. Chapter 3.3 will explain the threat identification with literature research and the sense making with expert knowledge.

3.1 INTERVIEWS WITH KEY STAKEHOLDERS

The main aim of the interviews was to get a detailed picture of threats, needs and security solutions in the three domains: cyber infrastructure, nuclear material and environment. This detailed picture helped us initially to set a thematic focus in each of the three domains and secondly to derive key factors for the development of the scenarios.

3.1.1 Selection of stakeholder

The first task was to identify stakeholders with expertise on understanding strategic, tactical, operational and societal needs. The basis for this identification was the list of stakeholders developed in Task 7.2 (see D7.2 "Stakeholder identification and analysis"). Thereby, identified stakeholders were selected from basically two different groups: Conventional security research end-users (e.g. Technical Relief Teams, Ministries of Civil Protection, etc.) and representatives from public and civil society organisations that are engaged in addressing societal needs (e.g. religious communities, civil rights groups, etc.).

We aimed at reaching a balanced mixture of both groups of stakeholders (e.g. governmental organisations, civil society organisations, etc.) as well as a balanced expertise of the selected thematic domains (i.e., cyber infrastructure, nuclear material and environment). We added a forth domain "general" – for all interviews from which we got inputs for all the three domains, nuclear material, cyber infrastructure and/or environmental issues and also about threats and needs on a more general level.

Overall 71 stakeholders were contacted – 27 of them agreed to be interviewed by us. Generally it can be observed that it is much more likely that stakeholders agree to do an interview, if the interview is conducted in their r mother language. Therefore the list of stakeholders was divided up among the members of the ETTIS consortium in order to cover different mother tongues. This meant that , organisations from the same country as the respective interviewers are a bit overly represented. In addition, unfortunately, it was not possible for the ETTIS consortium to convince stakeholders from Eastern European countries to be interviewed in English.

Many of the identified threats have a global significance (e.g. climate change, nuclear proliferation, cyber war), so that the results don't change much with the nationality of the interviewee. However, if future interviews were directed to detect local threats and needs, the project should be provided with a sufficient budget to be able to conduct interview in all relevant languages.

3.1.2 Development of an interview guide

To get an impartial picture of threats, needs and security solutions in the three domains we developed an interview guide with open questions to make sure that we do not restrict the answers of the stakeholders in any way. The interview guide is described in detail in chapter 3.1 of D4.1 "Threat Scenarios".

A general result of the interviews was that the majority of respondents didn't see the necessity to distinguish between "needs" and "solutions", although the members of the ETTIS consortium (interviewer) explained the difference at the beginning of the interview.

We observed that for the majority of the respondents the boundaries between "needs" and "solutions" were blurred. In most cases when asked for the societal needs the respondent explained what should be done in a more general way and when asked for solutions they put it in more concrete terms and gave examples.

3.1.3 Interview procedure

In order to ensure the rights and wishes of potential participants, the interviews were on a strictly voluntary basis, without risk, personal or otherwise for the volunteers.

Potential participants in the interviews have been given all the information that might reasonably be expected to influence their willingness to participate through an informative introductory letter and the declaration on data projection. Information about the aims and methods of the project was presented in a language easily understandable also by persons unfamiliar with research or the specific research topic. The information sheet as well as the data protection declaration was published in D4.1 "Threat Scenarios".

3.1.4 Interview results – Threats

In general it was observed that the majority of the respondents identified threats of different categories. On the one hand very high level threats such as climate change were mentioned. On the other hand, respondents also mentioned single event threats, such as e a terrorist attack on a nuclear site. Descriptions of the current situation out of which threats could develop (i.e., complexity of IT-systems, increase of mobile devices) were also pointed out. Additionally controversial technologies (e.g., genetically modified crops or nanotechnology) were mentioned as threats by some of the respondents.

Thus the interviews are not suitable as an only source to identify threats. Other methods such as weak signal scanning and also desktop research methods have to complement the results from the interviews to be able to derive a systematic list of future threats.

Although many of the respondents were quite reluctant to predict the development of the threats in the future, the consultation of experts is still one of the few methods available in areas which can't be reasonably computed (like meteorological events).

Thus we see expert interviews as good complementary method to identify future threats.

First results to societal needs

The interviews aimed to provide some initial insights on societal needs, specifically collect some explorative information on all the aspects from threats to needs and solutions associated to some examples of threats.

Most of the respondents mentioned rather general societal needs, such as education and awareness or good crisis management. On the other hand more specific suggestions such as new ICT systems with security by design or the withdrawal from the nuclear energy programme were also made. This meant that the identification of societal needs from expert interviews alone is rather difficult.

Thus, ETTIS uses the "needs" results of these interviews only as a correcting factor after using a methodical approach for the identification of societal needs (see chapter 4). However, the correcting input from the expert interviews is important to validate if our overall results are still in line with the perception of the experts.

Societal security solutions

When talking about solutions, some interview partners suggested technologies or technical guidelines (e.g. build-in security, high level of redundancy, detection systems), while others pointed out political measurements (e.g. international agreements, international cooperation), or general capabilities (e.g. well educated engineers, resilience of the society).

Within ETTIS the solutions are derived systematically in work package 6. The findings of the interviews provide a good way to validate the results of this work package and to include the point of view of the experts. However, possible differences in the findings could also emerge and, if this is the case, results shall be thoroughly examined.

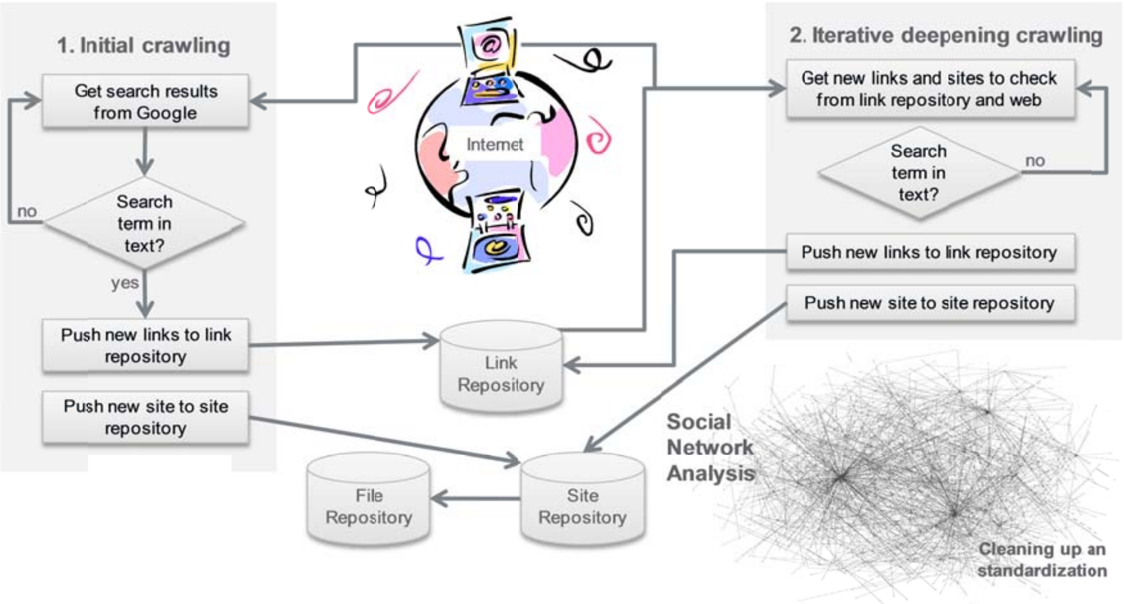
3.1.5 Conclusion

Overall, the expert interviews provide a good way to complement other more systematic methodologies to identify threats, needs and security solutions. Due to the different backgrounds of the experts, these three terms (threat, need, and solution) were associated with slightly different meanings. Thus, the answers of the interview partners fell into different categories or levels. Although the findings of the interviews can't be used as the only source to identify threats, needs and security solutions, they are still very valuable as initial input that can be used in an iterative process to corrective and fine tune findings from different methods. It is always better to have similar results from different methods, than having results from one method alone. In addition, the interview process allows how to stay in contact with the expert community.

3.2 WEAK SIGNAL MINING

As described in the D4.1, weak signal mining is based on internet scanning, with customized software. A starting point for the software scanning was that more than 99.9% of the files on web servers are irrelevant for our issue. So the idea was to identify only the relevant subset of the WWW in an effective manner. For this purpose, a threat identification agent (TIA) was developed at AIT. The following Figure 4 gives an overview of the overall system architecture of the TIA.

Figure 4: System architecture of TIA agent v0.1.


1. Initial crawling
Get search results from Google
Search term in text?
no
yes
Push new links to link repository
Push new site to site repository
Internet
Link Repository
File Repository
Site Repository
2. Iterative deepening crawling
Get new links and sites to check from link repository and web
Search term in text?
no
Push new links to link repository
Push new site to site repository
Social Network Analysis
Cleaning up an standardization

Source: ETTIS D4.1 report

3.2.1 *Process of weak signal scanning*

In the initial crawling stage the agent loads search results from a search engine like Google, which are considered as relevant for the search, i.e. in our case for threat identification. The agent then follows each of the links extracted by the search engine to a result list and downloads the corresponding text information. If this text contains the search string, TIA extracts title, keywords and main text, and notes the results in the site repository. It then extracts all links from this "relevant" site and adds them to the link repository.

In a second and final stage of data acquisition, the agent iteratively follows all extracted links, again extracts the site attributes and once more tests whether the main text of the site contains the search string. To prevent the agent from being drawn into "black holes"[3] for internet crawlers the agent will not download more than about 1000 documents from a single domain. All text results are grouped by domain, so that there is a consistent domain –text/date relation in the database. This database forms our data source for a topic map analysis.

[3] http://stackoverflow.com/questions/4512936/what-techniques-can-be-used-to-detect-so-called-black-holes-a-spider-trap-wh

Based on the downloaded dataset, the threat identification agent (TIA) uses hyperlinks from already identified community sites to find new community sites. By using hyperlinks, the agent makes use of wisdom of the crowds in a way that it uses links as expressions of trust from the source site to the link target site. As our potential text corpus on the internet contains hyperlinks, the text corpus can be thought of as a directed network, with authorities and hubs, in which an authority node is a site with a lot of inbound links, and a hub is a site with a lot of outbound links. Each node in the network has some text online, which can be used to form topic clusters.

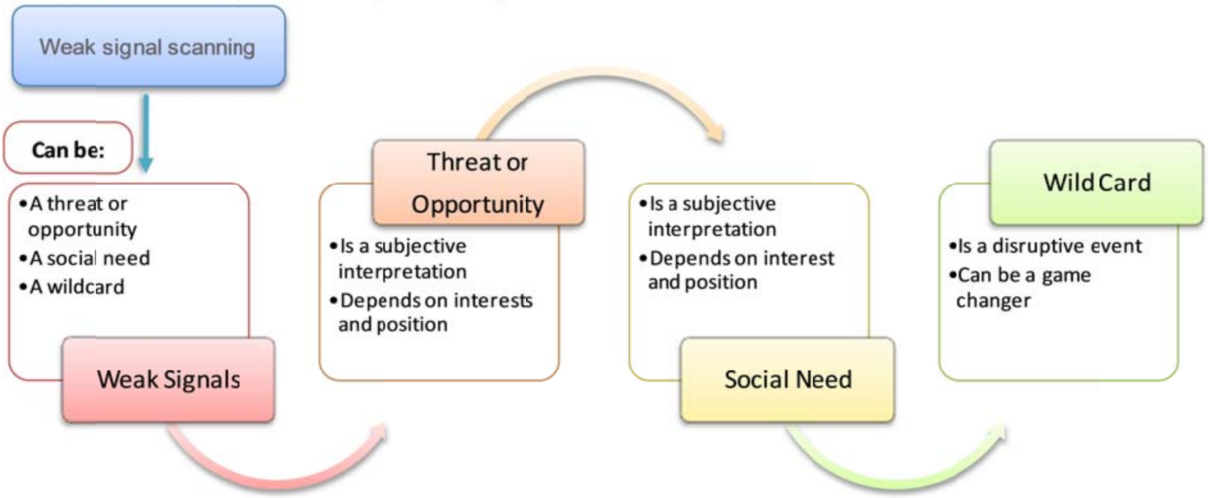
The clusters give an overview of the topics discussed in the community. As the whole text corpus is about future threats, the identified topics sum up the discussions about future threats. Finally, the identified discussions are manually analyzed to identify possible weak signals.

3.2.2 *Different types of results*

In text mining, the basic corpus, or more precise, the word frequency matrix of the basic corpus, is used as a kind of white noise for the analytical process. The TIA algorithm identifies weak signals, based on changes in the word frequency matrix, which are used as indicator for semantic weak signals.

However, these signals can either indicate a threat or an opportunity. They can also give hints to resulting future social needs, or can indicate wild cards. As the following graphic symbolises, it is a good practice in semantic analysis, to check first, whether there is a potential for a threat or opportunity, then check, whether there are hints to social needs in the topic and finally check, whether there is a potential for a wild card. This can be done by using expert knowledge. As a result, for the semantic analysis additional human research was necessary.

Figure 5: Analytical process in signal mining



Source: ETTIS D4.4 report

The following definitions, developed in WP4 were used to identify threats, opportunities, social needs and wild cards in the list of weak signals.

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

T**hreats** can be a warning that one is going to hurt or punish someone, they can be a sign of something dangerous or unpleasant which may be, or is, about to happen, or they can be a source of danger.[4] In each meaning, the following 3 essential elements are part of a threat:

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

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

Wild Cards are high-impact events that seem too incredible to believe.. Therefore they tend to be overlooked in long term strategic planning. Often it leads even to a decrease in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, "wild cards" refer to low-probability, high-impact events, as introduced by John Petersen author of 'Out of The Blue - How to Anticipate Big Future Surprises'.[5] However more important than probability is, that these topics are not well known and not part of the mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However for strategic long term planning and scenario development they are very important, as they increase the ability in scenario planning, to adapt to surprises arising in turbulent chaotic environments. In trend analysis, they point to trend breaks and tipping points.

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

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

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

The result of the weak signal scan was a list of about 70 weak signals for either harmful events, threats, trends, wild cards or social needs. Topics out of this list where later on used in the human threat identification.

3.2.3 Conclusion

Based on the presented method, it was possible to identify a remarkable number of weak signals for possible future threats and opportunities. In principle the internet is a suitable source for such a broad scanning. However, the findings from internet sources needs additional human reasoning and interpretation in order to extract more consistent and accurate insights. In the process of sense making all categories of future issues (threats, needs, wild cards, disruptive events and so on) became more accurate. . The precise knowledge about these different types of issues was not available at the beginning of WP4 Taking into account, that this knowledge is helpful in scanning the interneta repeated scan would lead to more precise results.

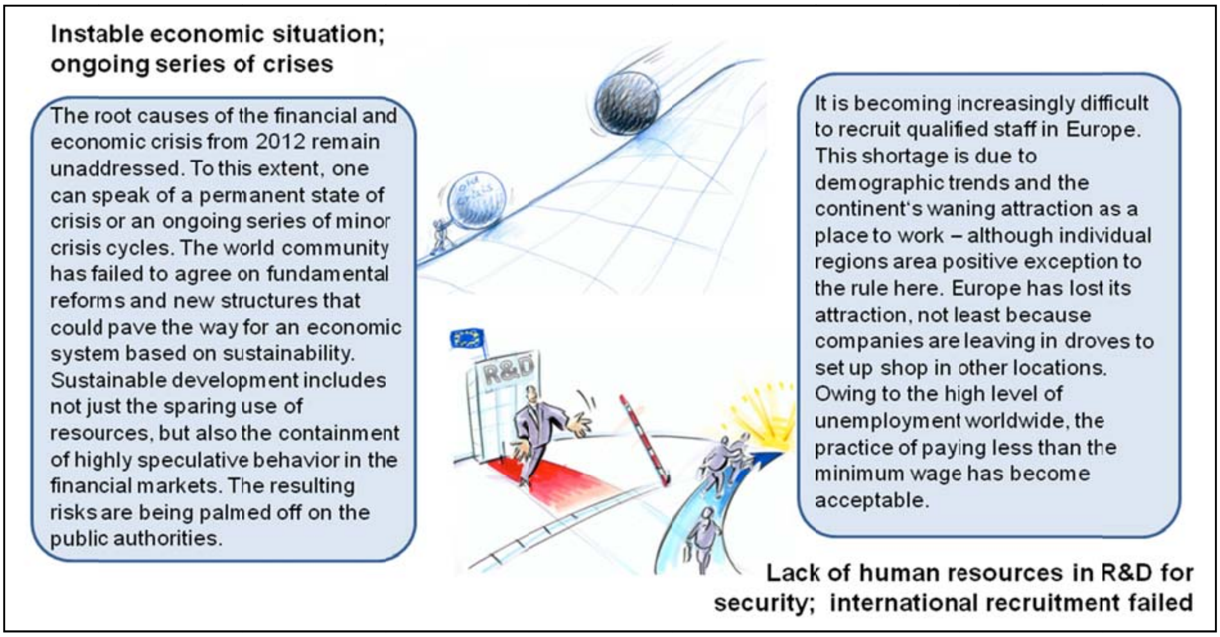
As a consequence from our experience with internet scanning, the scanning is very much driven by the definition of the search issue, which is reflected in the search strategy. Scanning activities will become better when expert experience in a specific domain is used to define the search strategy and a domain specific knowledge management is used to cluster the results. In general this implies, that repeated scanning can and should be used for iterative improvements in scanning activities.

3.3 ANALYSIS OF FUTURE STUDIES AND EXPERTS WORKSHOPS

The analysis, based on existing future studies and expert discussions in the focus group workshops and the validation workshop, delivered insights about the nature of threats which is twofold:

- There are threats with a procedural character, e.g. lack of safety requirements for handling nuclear material, instable economic situation or lack of human resources in R&D for security, see figure 6, and
- Threats with an event character, e.g. terroristic attack, natural disaster (see figure 7).

Figure 6: Threats with procedural character – an example



Instable economic situation; ongoing series of crises

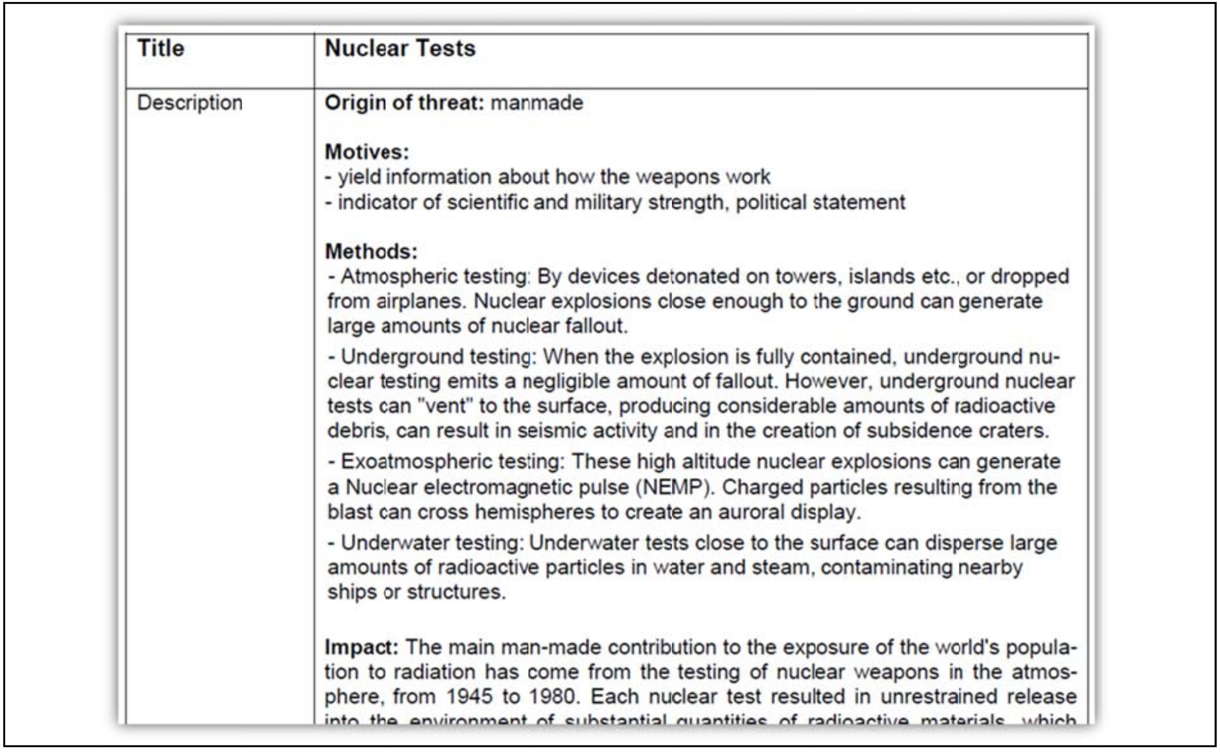
The root causes of the financial and economic crisis from 2012 remain unaddressed. To this extent, one can speak of a permanent state of crisis or an ongoing series of minor crisis cycles. The world community has failed to agree on fundamental reforms and new structures that could pave the way for an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

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

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

Source: ETTIS D4.4 report, Illustrator: Heyko Stöber

Figure 7: Threats with event character – an example



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

Source: ETTIS D4.4 report

3.3.1 The four-step-approach for human threat identification and interpretation

As the automatic the processes of threat identification, based on internet scanning, leads to a kind of raw list of threats, an additional process of sense making is required to develop a list of threats with more accurate definition. Based on the raw material, we developed in the following four step approach a list of threats with more accurate definition an description (see also D4.4):

- First step: Literature research (with focus on future studies);
- Second step: Focus group workshops;
- Third step: Structuring threats by the WP4 members;
- Fourth step: Scenarios validation workshop.

First step: The analysis of future studies

The analysis of the key work in future studies referred to threats at two levels: firstly to threats related to the global security issues (general security context) and secondly to the specific threats from the fields of cyber infrastructure, nuclear and environment:

(i) Regardless of the domain, a broad range of different threats such as the global financial crisis, under-investments in critical infrastructures or a lack of human resources in the field of security were considered.

(ii) There were also specific threats for each domain, such as wide spreading cyber IT technologies or the vulnerability of cyber infrastructure (cyber), a lack of safety requirements by handling the disposal and the transport of nuclear material (nuclear) and biodiversity loss or urbanisation (environment).

Second step: The focus group workshops

The focus of the focus group work was on identifying, prioritising and discussing the key factors and their future projections, which described future developments, that might be considered as threats or not, e.g. land use for agricultural production. The future projections A and B were discussed as a possible threats (see table 1). These were mostly threats with a procedural character.

Table 1: Possible threats contained in future projections – an example

	Future Projection A: Exacerbated soil degradation due to the agricultural production	**Future projection B: Use of land for agriculture is still most important**	**Future projection C: Effective use of land is getting more important**
Agriculture land in the EU	• Land use pattern determines the value of economic returns from agriculture and forestry production: The intensification of agrarian land and trying to use the land in the most efficient way results in leaching of soils. • Habitat and land use change still have largest global impact on biodiversity.	• Further converting of grassland and forestland to agriculture • Agricultural production for food consumption is still one of the predominant land-use activities across the globe and EU	• Targeted set-aside of arable land or maintenance of permanent pasture • Overarching land use concepts including food production, conservation of traditional landscapes, biodiversity “production” as well as creating new jobs in rural areas • Spatial planning, which improves local consumption patterns

Source: ETTIS this report

Third step: Structuring threats by the WP4 members

The focus of the third step was on prioritising and discussing the identified threats from each task by the WP4 team, while describing the selected threats in detail. This was a necessary step to handle the large number of identified threats by structuring them and finding a common level of a threat description. The prioritising was also based on the criteria presented above, such as relevance for the society, security and the EU. Furthermore, the threats with high impact were considered. A template was used in order to structure the stocktaking of threats (see table 2).

Table 2: Template for threat identification

Title	
Description	A threat is an event which has a specific **origin** (natural, manmade, accidental). It is caused by a mix of **methods** (actions, proceedings, techniques, instruments etc.) and **motive(s)** (financial, political etc.) **Impact**: What effects does this threat could cause? **Background**: Are there any additional information about this threat, like past and present developments? **Relevance in the future**: Is this threat also relevant in the future? How could this threat change *in* the future? How could this threat change the future?
Affected areas	In which areas this threat might be relevant? For which institution this threat might be relevant? What kind of influence might this threat have on these areas / institutions? What might be potential risks / opportunities?
Affected regions	For which regions / states might this threat be relevant? What kind of influence might this threat have on these regions? What might be the potential risks / opportunities?
Affected domain	Is this threat relevant for the context situation in general? Which domain might be affected (cyber infrastructure, nuclear, environment)?

Source: ETTIS this report

Fourth step: The scenario validation workshop

This approach was chosen in order to support active participation and dialogue from experts from different interested groups across and within the different domains. The discussions focused on the identification and the structuring of threats, and deriving societal security needs in a particular area based upon the participants' own experiences. The workshop process used a combination of different moderating activities, brainstorming as well as interactive presentations. The group discussions were oriented towards the following questions.

- What are the most relevant threats for cyber infrastructure, nuclear and environment?
- How relevant are these threats for the EU?

The discussions led in generally to a new structure of the threats in each domain and helped to clarify interdependencies among threats.

3.3.2 Conclusions

Summarizing the results of the work, the following points are obvious. (i) Firstly, the threat identification based on key work in future studies delivered similar results to the results of the focus group workshops and the validation workshop. Sometimes the findings identified the same threats, other time they pointed to threats that had strong similarities . This means that the expert discussions confirmed the results of the future studies . These results were useful as a first source of threat identification. Nevertheless, the discussions during the validation workshop often had a new focus, which enriched the descriptions of the threats. (ii) Secondly, some of the identified threats were reflected in the future projections, which were discussed by the participants of the focus groups. In addition as the validation workshop showed, it might be meaningful also to introduce these future projections as specific threats. (iii) Thirdly the exercise and all the related discussions have clearly shown key problems in the identification of emerging threats. This is manily due to teh following:

- Many **threats often reflect existing threats**, only carried out with different means.
- Though they are already well-known, **existing threats may change they occur** in many ways, like for example via different technical means, change of target groups or combination with other threats. On the one hand this underlines that “old” threats can very easily and fast become “new” threats. On the other hand this may **lead to different impacts** and consequently different needs.
- Emerging threats often **arise from an unforeseen combination of technologies, motives and possibilities**, which has similarities to other developments in the domain.
- **The different motivations**, i.e., intentional or unintentional, **may cause the same threats** with the same or similar impact. In some cases the intentional threats might cause additional mental damages, such as ideological, psychological damages, or may cause fear in society, which then affects the risk perception about threats in general.
- Prioritising of threats by criteria, such as relevance for the EU, society, security and their impact, does **not warrant the accuracy or completeness** of the collected threats.
- **Threats are not formulated on the same level**, which means, that some of the described threats are not the threat itself but the context, in which a threat may occur, such as political or societal context. Furthermore, threats could be formulated at a very different level of abstraction. On the one hand the definition could be very broad, on the other hand threats could be also very specific. Indeed, threats are mostly caused by other threats. Usually threats find themselves caught between policy and economic developments and among other threats with many interdependencies between these fields.
- The consequences of many threats might have a **high impact due to cascading effects**, independently of the threat location..
- Furthermore, there is a contrast between threats of high probability and low impact vs. threats of high impact and low probability. However the **probability was not explicitly debated**.

4 DISCUSSION OF SCENARIO APPROACHES

Chapter 4, 5 and 6 will discuss in detail the scenario methods used in ETTIS. This section starts with an overview of scenario approaches and introduces key technical terms, used in ETTIS scenario methods, for discussion of the ,. In the following, the scenario approach of

WP4 is discussed in detail and key insights relating to the grounding concepts have been put forward .

Chapter 5 will present the experience of scenario methods for need identification and in chapter 6 options for further developments with scenario methods in WP 5 are presented.

4.1 OVERVIEW OF SCENARIO APPROACHES

Traditionally scenarios are built for two reasons: exploration and decision support. Scenarios explore the future and identify several future perspectives, thus provide a background of decision making (Schomaker 1995, p. 25). Considering a range of possible futures, decision makers will be better informed and their decisions based on this knowledge will be more grounded. Moreover, by constructing scenarios, decision makers win awareness of the variety of future possibilities, uncertainties in surrounding environment, indicators of discontinuities and the way societal processes influence one another. While they "face" possible events which might happen in the future, they expand their mental models into developments not yet thought and start to shape the future by introducing appropriate measures in the present. . By doing so, they prepare themselves for discontinuities in today's world. Scenarios cannot predict the future, but show the variety of possible futures. Thus, they are not a tool showing if an event occurs, but a tool helping to manage the situation which might happen.

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

- Step 1: Identification and selection of the influencing factors, in this report called the key factors;
- Step 2: Development of future assumptions for the selected factors, in this report called the future projections;
- Step 3: Bundling the future projections to different and consistent scenarios.

There is no single approach to bundle the future projections to scenarios. Instead a wide range of qualitative and quantitative scenario approaches exist, which are discussed in the scenario planning literature and applied to different purposes. Generally the scenario building is based on intuitive or algorithmic (quantitative) methods (Dönitz 2009, p. 24-25, Amer 2013, p. 26-27).

The intuitive logics school comprises approaches which are strongly based on plausibility and explanation of the causal processes, connections and logical sequences underlying developments (Wright et al. 2013, Wilkinson et al. 2013). An example of this group of methods is the best-guess approach. Purely intuitive assumptions (best guess) about which developments of each key factor are most likely in the future are used to assign future developments to the scenarios. The combination of the most likely future projections results in a so-called “mainstream” scenario; from the combination of the less probable future projections at least one “understream” scenario is derived (Möhrle, Müller 2002, p. 79). In some cases this is a very useful approach, e.g. to create normative scenarios or extreme scenarios, particular in security. However, in complex systems with many interdependencies among key factors it may happen that the internal consistency and plausibility get lost. Therefore it is recommended to applying algorithmic computer-assisted methods, such as consistency analysis or cross-impact analysis (Mißler-Behr 1999, p. 325). The aim of the algorithmic approaches is to limit the total number of all projection bundles. There is a distinction between two selection steps in which the number of all bundles is gradually reduced.: After a pre-selection is done, the so-called classification methods, i.e., cluster analysis or multidimensional scaling, are used to determine the final projection bundles whose number is often defined by the user. The consistency, diversity and stability of the later scenarios are mostly used as evaluation criteria for the selection.

The concept of the scenario development by using quantitative approaches, in particular to bundle the future projections, will be discussed in more detail in chapter 4.1.1. The decision on the selection of one approach depends to a great extend on the purpose of the scenario building, thus scenarios are mostly a starting point of further analysis. Some possibilities of the applying of the scenario results are presented in chapter 4.1.2.

4.1.1 Quantitative methods of scenario building

Since the early 1980s new algorithmic methods for the evaluation and selection of bundles with future projections have been proposed. Basically, there is a difference between approaches that are based on the consistency or on probabilities. However, some approaches are based on a combination of both parameters. This is broadly discussed in the scenario literature. An overview of the relevant works is proposed by Dönitz (2009, p. 25, 27) as well as by Amer (2013, p. 29-31). Dönitz describes the following main approach groups proposed by Mißler-Behr (1999, S. 319-324; 1993, p. 94-116): (i) enumeration and branch-and-bound algorithms; (ii) equation systems and optimization models; (iii) simulation methods. The first and last approach groups are presented below and their advantages and disadvantages considered. The equation systems and optimization models are the focus of the further explanations, since often they cannot be solved due to a big number of variables and constraints.Therefore they are less relevant for realistic problems. Furthermore, scenarios are often combined and integrated in various ways with other methods (Kosow et al. 2008, p. 61), such as modelling to quantify scenarios and consider different time horizons (see description below); Delphi surveys for setting a basis for the future projections or evaluating scenarios; and road mapping to operationalize scenarios for the strategic planning.

Enumeration and branch-and-bound algorithms

The general procedure of the enumeration and branch-and-bound algorithms is based on the consistency analysis.Based on the estimated consistency values in the consistency matrix (see chapter 5.2), the entire scenario space is displayed in a tree structure. All possible combinations of future projections (bundles) are built and evaluated according to their overall consistency. The higher the average consistency, the “better” is the bundle. In order to reduce the number of bundles following selection criteria could be applied (Dönitz 2009, p. 27):

- Increasing the average consistency of a bundle: A defined minimum consistency level should be reached.
- Reducing the number of partial inconsistencies: The increased number of partial inconsistencies in a bundle leads to its exclusion. The lower consistency values could not be compensated by the higher values.
- Reducing the number of high inconsistencies: The bundles which include the high inconsistencies are not considered in the selection process at all.
- Reducing using the diversity: The selected bundles with future projections are not only consistent, but they differ also significantly from each other (see chapter 4.2).

The main advantage of the enumeration and branch-and-bound algorithms is the limited amount of input variables, in this case, required for ? consistency values. Furthermore a large number of key factors and future projections can be processed. The user can directly influence the selection criteria which might change the quality of the results. The main criticism concerns building scenarios without consideration of probabilities.

The consistency analysis provides a relatively simple approach for determining the scenarios and is easily comprehensible by the involved persons, e.g. users, involved experts or clients. Although the estimating the consistency values is very time consuming and complex (Dönitz, Möhrle 2006, 2009), compared with other scenario building methods, such as the cross impact analysis, the consistency analysis significantly requires less efforts. Furthermore, the importance of consistency is emphasized as an essential characteristic of scenarios (Weimer-Jehle 2006, p. 335; Lindgren, Bandhold. 2003, p. 31; Schlake 2000, p. 79; Zinser 2000, p. 46 and Mißler-Behr 1995a, p. 45).

One of the criticisms of the consistency analysis which has been not taken into account by the most authors is related to the question whether the requirement for the consistent pictures of the future does make any sense since the present already contains many inconsistencies. A consistency analysis of the present would eventually lead to the conclusion that some serious inconsistencies exist (Dönitz 2009, p. 244). From a methodological point of view a scenario describing such a combination would be sorted out from further analysis. This leads to the question: Is building consistent scenarios realistic and useful at all?

This question has been taken up by Postma and Liebl (2005, p 171) who propose a kind of in-consistency analysis, in addition to the consistency analysis. They focused their analysis on highly probable scenarios which were high inconsistent at the same time. The challenge for the scenario team was to create scenarios which included paradoxical developments or events. Through the explanation of the main contradictions, the interactions between the relevant factors were identified and discussed.

Despite these reflections, consistency analysis does have its raison d'être, as the developed scenarios are not exempt from all inconsistencies (Dönitz 2009, p. 244-245). By applying consistency analysis not all, but only the major inconsistencies are excluded. Even after applying consistency analysis scenarios still include some inconsistencies. (i) Firstly by taking the partial inconsistencies into account; (ii) secondly by considering developments which are not included in the consistency check (developments without an alternative which flow into every created scenario); and , (iii) thirdly by taking into account the criterion of diversity which is as relevant as the consistency criterion and mostly in conflict with it.

Simulation methods

The simulation methods include approaches that examine what kind of impact the occurrence or non-occurrence of one future projection might have on other future projections. This is termed as so-called direct or indirect cross-influences (cross impacts) of the future projections. To evaluate the impact an adaptation function is used and the problem is solved by simulation. Simulation methods generally try to replicate the reality in a model and to gain insights by repeatedly running the model. The aim of the calculation in the illustrated case is the selection of one single scenario in one simulation run, starting with one future projection. Those scenarios that are the most frequently selected as a result of all simulation runs are included in the final scenario set. The two following examples should illustrate the procedure (Dönitz 2009, p. 28-29):

- One example of the cross impact analysis is the static-causal BASIC procedure (Batelle Scenario Inputs to Corporate Strategy). The probabilities of the future projections flow as input data into the analysis. These probabilities are estimated by experts according to a defined scale. While estimating the probabilities the experts try to answer the following leading question (Geschka, Reibnitz 1981, Annex I, p. 6): What is the impact of the occurrence or not-occurrence of one future projection on the occurrence probability of another future projection? The estimating process is similar to the estimating of the consistency values (see chapter 5.2). However, there are twice as many values to estimate as in case of the consistency analysis. The process works as follows: One of the future projections is randomly selected. The effects of the occurrence or non-occurrence of this future projection to all other future projections are simulated. This procedure is repeated until one scenario is identified. The selection criterion is the frequency in the simulation process.
- The deterministic dynamic concept of Kane is an example of the dynamic approaches of the scenario building (1972, p. 129-142). The Kanes simulation (KSIM) was originally developed to derive qualitative information from quantitative statements about dynamic processes (Hofmeister 2000, p. 109). Due to the similar objectives of this approach and the cross impact analysis KSIM is also applied in the scenario analysis. Basis of the simulation represents an interaction matrix, similar to the influence matrix (see chapter 4.3.2). In the interaction matrix for each future projection is checked to which extent it is influenced by every other future projection and vice versa. During the simulation the influence values from the previous period are corrected by the mutual influences. The total impact on a future projection varies from a period to a period because the current value is recalculated every time (dynamics). The result of the simulation is a set (bundle) of future projections with the specific, previous defined values (determinism). To generate additional bundle a new simulation is run based on modified dependencies or even initial influence values.

  The simulation methods fit problems with a high number of the key factors and the future projections. However, the gaining of the input data is the main challenge (Gierl 2000, p. 65-66, Götze 1993, p. 181). The number of values which have to be estimated is approximately twice as large as in the case of consistency analysis. This requires high efforts invested by users and included experts (Brewer, Weber 1986, p. 637). Furthermore, the user is not able to control the quality of the results (Mißler-Behr 1995, p. 53), as the quality of the selected bundles is determined only by the frequency. There is no guarantee that these bundles are consistent, plausible or representative as well.

Modelling

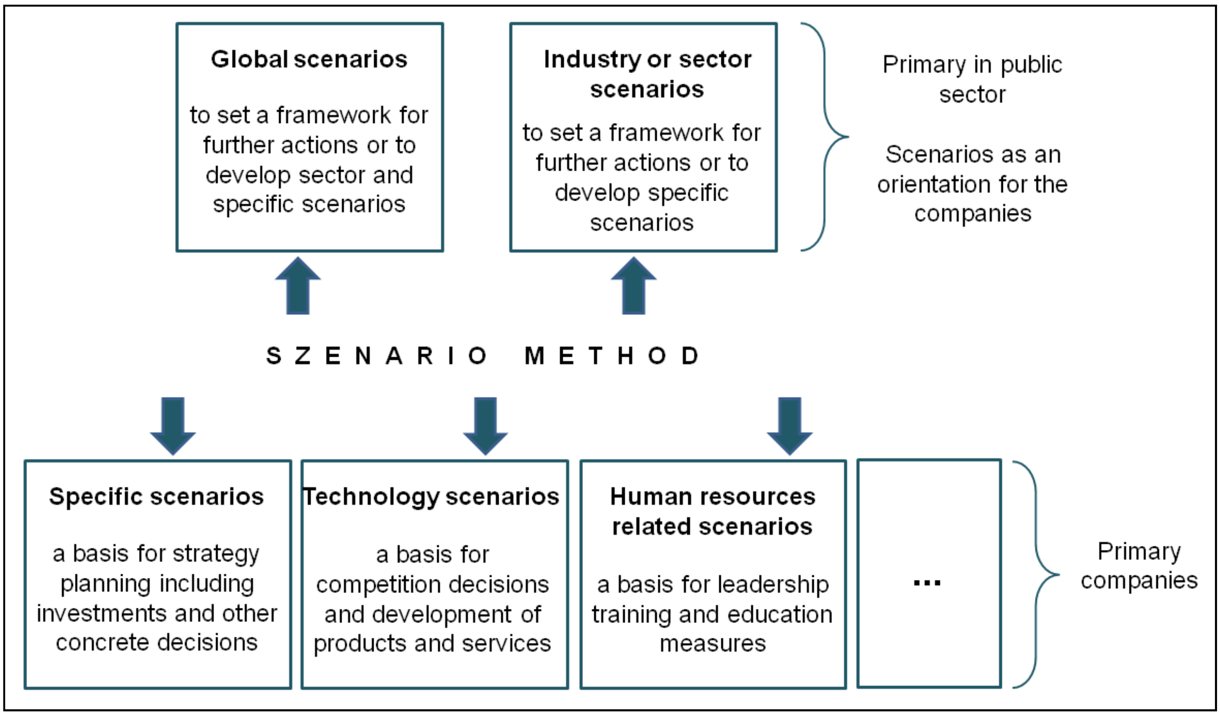
Modelling is mainly used for the systematic analysis of complex relationships. The behaviour and interaction of different variables is simulated, mostly via IT tools.. In the future research simulation models are used to represent non-linear dynamics, and often to quantify variables and their effects. In the context of future research there are three main types of models (Kosow et al. 2008, p. 61): (i) System dynamics models, usually used to quantify variables; (ii) agent-based modelling to simulate the behaviour of individual actors in the interaction; (iii) specific qualitative models to represent the uncertainty of the future. Recent research works have been focused more on the integration of qualitative and quantitative models to a one hybrid approach.

The variety of possible future projections in scenarios and the challenge to communicate the results of scenario processes might lead to an integration of scenarios and models. Therefore on the one hand the qualitative scenarios are often translated into models and quantified. On the other hand there is also a "translation" of model results into scenario stories. There exist also approaches in which narrative scenarios (so-called story-lines) are developed in several stages. The stories flow into models and are translated into narrative scenarios again to validate scenarios and models as well (Kosow et al. 2008, p. 61). This approach is also known as the "story-and-simulation" approach (SAS).

4.1.2 Possible applications of scenarios

Scenario method is a flexible planning tool with regard to the subject of the investigation as well as to the depth of analysis, thus it can be used in many ways and for different proposes. There are two types of client and initiators of scenario studies (Geschka et al., 1997, p. 58): (i) The public sector is interested particularly in scenarios of different industries and sectors, like transport or energy, as well as in global scenarios. The global scenarios and the industry scenarios play an important role, because they serve as a kind of framework conditions for further actions, like investment decisions or decisions about research priorities (Fink et al. 2000, p. 48); (ii) Companies develop mainly company-specific scenarios, including technologies and market developments, but also the surrounding environment. The results flow directly into the strategic planning, to evaluate the existing strategic options or develop new strategies (O´brien, Meadows 2013, p. 644-645). Moreover, they build normative scenarios to create their own vision and mission. There are also some further application of the scenario method, e.g. in human resources development (see Figure 8).

Figure 8: Possible applications of scenarios


Global scenarios
to set a framework for further actions or to develop sector and specific scenarios
Industry or sector scenarios
to set a framework for further actions or to develop specific scenarios
Primary in public sector
Scenarios as an orientation for the companies
SZENARIO METHOD
Specific scenarios
a basis for strategy planning including investments and other concrete decisions
Technology scenarios
a basis for competition decisions and development of products and services
Human resources related scenarios
a basis for leadership training and education measures
...
Primary companies

Source: Dönitz 2009, p. 39; based on Geschka et al. 1997, S. 58

In most cases scenarios are a starting point of further activities and not the aim in itself. Depending on the scenario purpose scenarios can be incorporated into the strategic planning in different ways. There is no universal model for that. The results of a scenario process can be used on the one hand to design the policy; on the other hand they can be integrated in different ways into operational and strategic planning. However the authors agree on one point: The use of scenarios in strategic planning is only useful if it is done as part of a continuous process. It is not enough to develop scenarios and identify paths into the future. The future assumptions must be continuously monitored and modified if necessary (Dönitz 2009, p. 40-41).

Dönitz (2009, p. 42-44) summarise the benefits and criticism on scenarios by using three criteria:

- The primary functions of the scenario method relating to its objectives, such as the creation and presentation of alternative pictures of the future, pointing out the relevant risk factors and uncertainties as well as future opportunities.
- The desirable or non-desirable "side effects" which do not belong to the primary objectives, but refer for example to the learning effects that may arise in the application of the scenario method, e.g. kick off for future dialogs or extension of the perception. The importance of these "side effects" should not be underestimated.
- The methodology of scenarios in comparison to other forecasting methods, such as the systematic approach or the high transparency of the scenario process.

One important “side effect” of scenarios is their use as a communication tool, thus they create a common language that can be used to discuss complex matters. The results of scenario processes should be presented in a transparent and comprehensible form with regard to both the content and the process itself, regardless of whether they are addressed to public, politics or business or to professional communities (Steinmüller, Schulz-Montag 2003, p. 35).

Scenarios should tell a story which is remarkable, convincing, logical and plausible. They should have a descriptive title that transmits the essence of the events described in the scenario. Well formulated qualitative scenarios meet these requirements to a large extent if they are clearly, easy to understand, consider aesthetic and affective moments or illustrate values and thus facilitate decision-making and communication processes (Steinmüller 1997, p. 62-63). Sometimes it may be necessary to reinforce the communicative side of scenarios by interpreting them in literary way or by the implementation of multimedia, photographs, diagrams, tables or graphics (Shell 2008, p. 60).

However, the benefits of scenario stories could easily turn into disadvantages, if they are not well-founded by the methodology. The clearness can lead to the suggestiveness. An illustrative, but unilateral scenario can direct the further process in a certain direction, leading to a constricted view of the problem. The high flexibility of the scenario process and the literacy of the scenario text are accompanied by an equally high manipulability. The explicit consideration of values linked with a lack of transparency lead to a blurring of the boundary between descriptive and normative, especially when the scenario is literary success (Steinmüller 1997, p. 63).

Mostly it is not necessary to create scenario stories, when scenarios are incorporated into the strategic planning and support the strategic decision-making. The own scenario experience shows, that the decision makers mostly prefer the key factors and future projections themselves. However, this does not apply to the scenarios which build the basis for the corporate vision or mission statement or are used in corporate communication (Steinmüller, Schulz-Montag 2003, p. 35-36).

The requirement for creativity refers not only to the way of writing, but also to the content of scenarios, the global context in which scenario evolves, implications of each one on the investigated area, challenges, opportunities and threats (Brabandere, Iny 2010, p. 1511). The stories mostly involve a temporal sequencing of events and developments that can be organise chronologically or thematically, but they should follow an internal logic that makes them plausible (Bowmann et al. 2013, p. 737).

4.2 METHODICAL CONCEPT OF SCENARIOS IN ETTIS

Scenarios within ETTIS describe alternative developments as framework conditions for occurring future threats (WP4) and their handling (WP5). The overarching aim of the scenario development in ETTIS is twofold:

- to develop threat scenarios across different contexts in different test fields, called domains: cyber infrastructure, nuclear and environment. They describe the relevant future developments and offer different future perspectives for identifying future option spaces. They help to identify the main actors and their motivations by including different dimensions, like the society, policy, research or industry. Within the ETTIS project scenarios serve as a base for the identification of future possibilities which are solutions related to societal security needs;
- to make a significant contribution to the methodological approach and model for a revolving process of security research priority setting which will be developed and tested in ETTIS.

The scenarios are useful for **analyzing how different threats affect society across different plausible futures** described in the threats scenarios. They enable the discussion of different inter-linkages between threats and needs in relation to societal, political, technological and economic issues. These results flow directly into WP5. (i) Firstly, they are used **to evaluate what kind of solutions may be needed** or developed to meet these future needs depending on the different framework conditions in the different scenarios. The proposed solutions might have both, a technological and non-technological nature.(ii) Secondly, the results are used **to prioritize the solutions**: Are they robust towards the different scenarios of one domain? Are they robust towards the different domains? Furthermore scenarios also point out the possibilities in order to develop a rationale for including or prioritizing research topics in a European strategic security research agenda in WP6.

The scenario development within WP4 proceeded at two levels: At the first level, **four context scenarios** were created and, at the second level, **four threat scenarios** for the domains cyber infrastructure, nuclear and environment were built following the principle of the context scenarios. All scenarios are described in detail in D.4.4. The terms context and threat scenarios were discussed in D3.1. The **context scenarios** have an overarching relevance for the field of security (e.g. EU policy, demography, trends and drivers in technology) and are equally important for the domains of cyber infrastructure, nuclear and environment. The context analysis also includes the identification of emerging trends and global developments. The **threat scenarios** describe the most important aspects or threats in each domain and shall apply only to a particular domain (e.g. quantities regarding nuclear waste or global safety norms for dealing with nuclear material).

Thus, these scenarios include threats with mostly a **procedural character** (e.g. a lack of safety requirements or insufficiently providing information about nuclear risks). An additional analysis of threats with an **event character** (e.g. terroristic attack or natural disaster) was conducted (see chapter 3). In order to identify **societal security needs** (a term also discussed in D.3.1)**,** a further analysis was carried out to investigate what happens when a threat occurs in different scenarios (table 3; see also chapter 5 and the term discussion in D.3.1). The context and the threat scenarios describe a wide spectrum of various future possibilities which have different implication on arising societal needs (see D.4.5) and proposing solutions based on different capabilities which could exist or could be missing in these scenarios.

Table 3: Need identification, based on threats occurring in scenarios – an example

	Context A: Scenario “Regulating sustainability”	**Context B:** Scenario “Awareness without action”	**Context C**
Threat 1: Climate change (greenhouse effect/ global warming)	**Societal need:** ▪ Efficient common international mitigation policy and agreements; ▪ Identification with the same goals and actions; ▪ Stable climate; ▪ Support the adaption to climate change	**Societal need:** ▪ Not reducing of the human life quality; ▪ Spread the knowledge about climate change and its consequences in society	...

Threat 2: Food (in)security	**Societal need:** ...	**Societal need:** ...	...
...	…	...	...

Source: ETTIS this report

The considered time horizon in ETTIS differed across the different domains. For the cyber domain a shorter time horizon has been set (5-10 years), opposed to the nuclear and environment domains which use a longer time frame (10-15 years). This approach was chosen as the cyber domain is characterized by technologies with shorter and more dynamic innovation cycles and is therefore subject to constant changes. 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 to different timeframes, the experts participating in the two workshops identified likewise similar context factors to be the most influential.

The scenario development conducted in ETTIS contained the three main steps described above: (i) Step 1: Identification and selection of the influencing factors, called the key factors in this report; (ii) Step 2: Development of future assumptions for the selected factors, called future projections in this report; (iii) Step 3: Bundling the future projections to different and consistent scenarios. Moreover, it relied strongly on the workshop approach. During the workshop the quantitative and qualitative factors were processed alongside each other and integrated into scenarios. Building on different levels of background research, conducted in the different tasks in WP4, which varies in its comprehensiveness, the first important sub-step was to develop the future assumptions. Taking into account the basic principle of approaching the future with an open mind, in the sense of “thinking the unthinkable”, a “leap into the future” is often possible in the form of a workshop, which is initially only concerned with sketching a mentally or argumentatively imaginable world (Seidl/ Werle 2011, p. 292), for which the necessary sequence of steps or a roadmap are not yet known. The development of assumptions about the future (future projections) is combined with creativity methods, e.g. brainstorming or brainwriting (Brunner 2008, p. 124-143), in order to ensure that the assumptions do not simply reflect a continuation of past trends. Additionally to brainstorming and brainwriting which were applied in ETTIS, the focus group workshops were opened with presentations which provided an outlook on the future , sometimes even a provocative one. Furthermore, external experts were involved in the process of further scenario developments in order to promote the expansion of perception (see D.4.3 and D.4.5).

The objectives of the scenario development process are listed in the figure below (see figure 9). These objectives were also embedded in the ETTIS approach.

Figure 9: Objectives of the scenario development process

(1) **Extend the perception**: thinking beyond established pathways

- Future study analysis in the considered field
- Expert identification and selection
- Identification and discussion of relevant factors

(2) **Handling complexity**: Separately discussion on the key factors

- Factor evaluation
- Selection of the key factors for the further discussion

(3) **Future alternatives**: Considering alternative developments for each key factor

- Identification of uncertainties
- Development of the future projections which describe possible developments of the key factors

(4) **Bundling of future projections**: Building of different scenarios with a high internal consistency and high diversity between each other

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

Source: Fraunhofer ISI; Illustrator: Heyko Stöber

The bundling of possible developments in order to build different scenarios (4, figure 9) is based on two main criteria: the internal consistency of each scenario as well as its plausibility and the diversity among the scenarios (see also chapter 5.2). Further criteria which were taken into account were the transparency of the results and the relevance for the purpose in ETTIS, the deriving of societal needs (considering a wide range of threats). This happened according to such criteria like the utility (scenarios must meet the specified purpose) and the intelligibility (scenarios must to be comprehensible and transparent, see Steinmüller 1997, p. 63; Durance, Godet 2010, p. 1488). However the plausibility and the consistency (credibility) are the most important aspects regarding the scenario validation (Steinmüller 1997, p. 63; Amer et al. 2013, p. 38; an overview of the scenario validation criteria is presented on p. 36-37).

4.3 SCENARIO DEVELOPMENT IN WP4

The aim of the scenario development in WP4 was to develop the scenarios and to identify the societal security needs associated to these scenarios. This includes, as a preparatory step, the analysis of existing future studies works within the domains of cyber infrastructure, nuclear and environment, the conducting of the focus group workshops to gain expert opinions about the most relevant aspects in the three domains and their future development (see D.4.3), and the consistency workshop to build scenario drafts and discuss them within the consortium and with end-users (see D.4.4). The main results of these activities were the identification of threats and trends, which provided the basis for the development of scenarios as well as a deeper understanding of the contexts of the threat scenarios. The final activity was the scenario validation workshop to discuss scenarios, threats, while identifying societal security needs which are the basis for the development of scenarios dependent solutions.. Results from this should feed into WP5.

The scenario development was conceived as an iterative process of the research exploratory activities:

- Research-based deriving of the **key factors** and their **future projections** by the analysis of different future studies and the focus group workshops (cyber infrastructure and nuclear) as well as the survey (environment), (steps 1 and 2, see chapter 4.1);
- Consistency analysis and influence analysis to build the **context scenarios** (Step 3, see chapter 4.1);
- Linking the context scenarios with key aspects within the domains
- Building the **threat scenarios** (consistency workshop) (step 3, see chapter 4.1).

The approach of the future study analysis and the focus group workshops is described in chapter 4.3.1. The results put forward a solid basis for developing context and threat scenarios. These two levels of scenario building, the context and the threat scenarios, are describe in detail in chapters 4.3.2 and 4.3.3. A critical review of the scenario development in ETTIS is provided in chapter 4.3.4.

4.3.1 Research based deriving of the key factors and their future projections

In the context of the future study analysis a wide range of secondary sources was systematically analysed, such as literature related to the security in general as well as various future studies and research works with focus on future developments and related to cyber infrastructure, nuclear and environment. These documents represented the views of different organisations, e.g. think tanks, other NGOs, research institutions and academia. Although the focus was mainly on the European-funded research projects, also projects outside the EU were analysed (see D4.3 and D4.4).

The results of the future study analysis were used as basis for the expert based discussion in the focus group workshops (cyber infrastructure and nuclear) as well as for the development of the interviews and the survey (environment). Experts representing the following fields were invited to attend the focus groups workshops as well as answer the survey (see D4.3):

- The focus group workshop on the future of cyber infrastructure addressed i.e. aspects related to e 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 dealt with nuclear power plants, use of nuclear material, nuclear accidents, waste management risks and dumping of hazardous waste.
- Interviews and survey for the domain environment primarily focused on the environmental degradation, i.e. biodiversity loss and invasive alien species, water pollution, land use and pollution, deforestation and soil erosion, population growth as

well as potential conflicts related to the resource scarcity, resource distribution and climate change.

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

The focus group workshop approach was chosen in order to support active participation from and open dialogue with experts from different interested groups. The discussions focus on different future developments in a particular area based upon the participants' own experiences. The workshop process is a combination of different moderated activities, brainstorming as well as input presentations. 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.

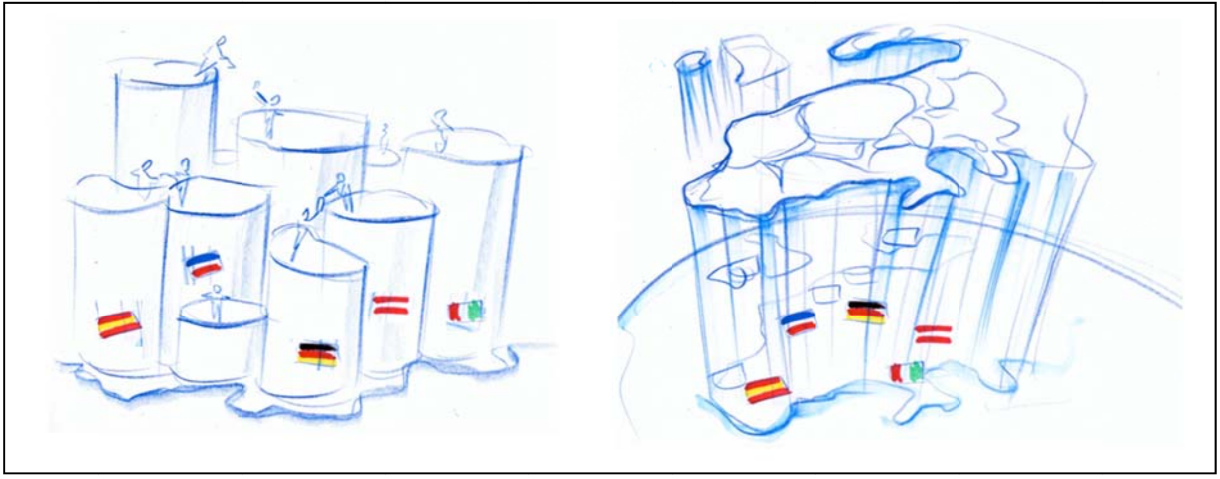
The relevant aspects in the context and the threat scenarios are described using so called **key factors**. The **key factors in the context scenarios** have an overarching relevance for the field of security (e.g. EU policy, demography, trends and drivers in technology) and are equally important for the domains cyber infrastructure, nuclear and environment. The context analysis also includes the identification of emerging trends and global developments. The **key factors in the threats scenarios** describe the most important aspects or threats in each domain and shall apply only to a particular domain (e.g. quantities regarding nuclear waste or global safety norms for dealing with nuclear material).

The possible future developments of the key factors are described in the **future projections**. In the focus group workshops (see D4.3) experts discussed whether only one possible future assumption should be made or whether there are conceivable alternatives. Alternative assumptions were developed for all key factors. The key factors themselves are all considered within the scenarios by the different projections; in turn, the diverse future projections of the key factors are needed for building scenarios which differ from each other. Future projections were identified for the contextual as well as for the threat related key factors. The following example shows the dependency between key factors and projections: For example, two possible developments might be assumed for the key factor "Overall development of the EU" (see figure 10) at the context level:

- "EU of Institutions": The integration of the European Union was already stagnating in 2013. During the economic and financial crisis, the member states principally looked for individual solutions rather than pursuing a joint European strategy. This trend is still continuing: the member states focus their attention primarily on optimizing their own economies and joint efforts are limited to security and foreign policy at most.
- "EU of Citizens": The integration of the European Union is largely complete. Europe is now competitive with other regions due to a jointly agreed and closely coordinated

economic policy, joint security interests and a unified position in other areas. The political integration resembles the societal integration. The population feels a connection to Europe due to the emergence of an integrated European economic and employment area.

Figure 10: An example for a key factor and its future development



Source: Behlau et al. 2010; Illustrator: Heyko Stöber

4.3.2 *Context Scenarios*

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

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

- Prioritizing the context key factors with regard to the relevance for the domains and security: The focus group workshops on cyber infrastructure and nuclear as well as interviews and survey for environment;
- Developing future projections: The future study analysis and the focus group workshops;
- Building scenarios: The consistency analysis (internal workshop in core team) as well as the consistency workshop for consortium members;
- Influence analysis to identify driving forces and scenario discussion: The consistency workshop.

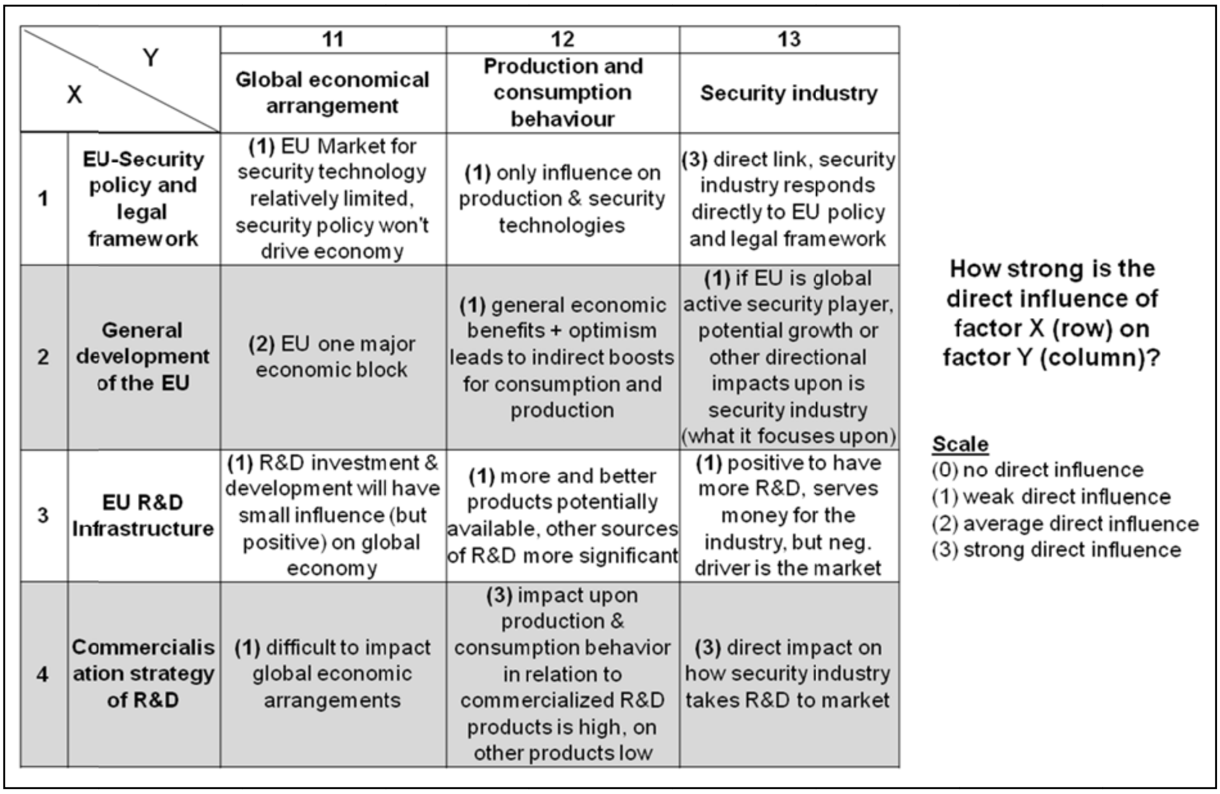
Based on these results a list of 17 global security related key factors was compiled for the context scenarios and the future projections for global key factors were gained. For each key factor two to four future projections were identified.

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

In the influence analysis each factor was checked to which extent it is influenced by every other factor and vice versa (see figure 11). Another part of the task was also to record in writing the rationales behind the assigned points. A scale of 0 to 3 has been used: 0 = no direct influence, 1 = weak direct influence, 2 = average direct influence and 3 = strong direct influence. Finally, all the points were totalized per factor in the columns "∑ passive" for the level of influence by the other factors and "∑ active" for the level of influence of the factor on the other factors. Table 4 shows a list of the 17 context factors and the sum of active and passive influence points that were allocated during the consistency workshop.

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

Figure 11: Influence matrix - future projections – an example



Y X		11	12	13
		Global economical arrangement	Production and consumption behaviour	Security industry
1	EU-Security policy and legal framework	(1) EU Market for security technology relatively limited, security policy won't drive economy	(1) only influence on production & security technologies	(3) direct link, security industry responds directly to EU policy and legal framework
2	General development of the EU	(2) EU one major economic block	(1) general economic benefits + optimism leads to indirect boosts for consumption and production	(1) if EU is global active security player, potential growth or other directional impacts upon is security industry (what it focuses upon)
3	EU R&D Infrastructure	(1) R&D investment & development will have small influence (but positive) on global economy	(1) more and better products potentially available, other sources of R&D more significant	(1) positive to have more R&D, serves money for the industry, but neg. driver is the market
4	Commercialisation strategy of R&D	(1) difficult to impact global economic arrangements	(3) impact upon production & consumption behavior in relation to commercialized R&D products is high, on other products low	(3) direct impact on how security industry takes R&D to market

How strong is the direct influence of factor X (row) on factor Y (column)?

Scale
(0) no direct influence
(1) weak direct influence
(2) average direct influence
(3) strong direct influence

Source: ETTIS this report

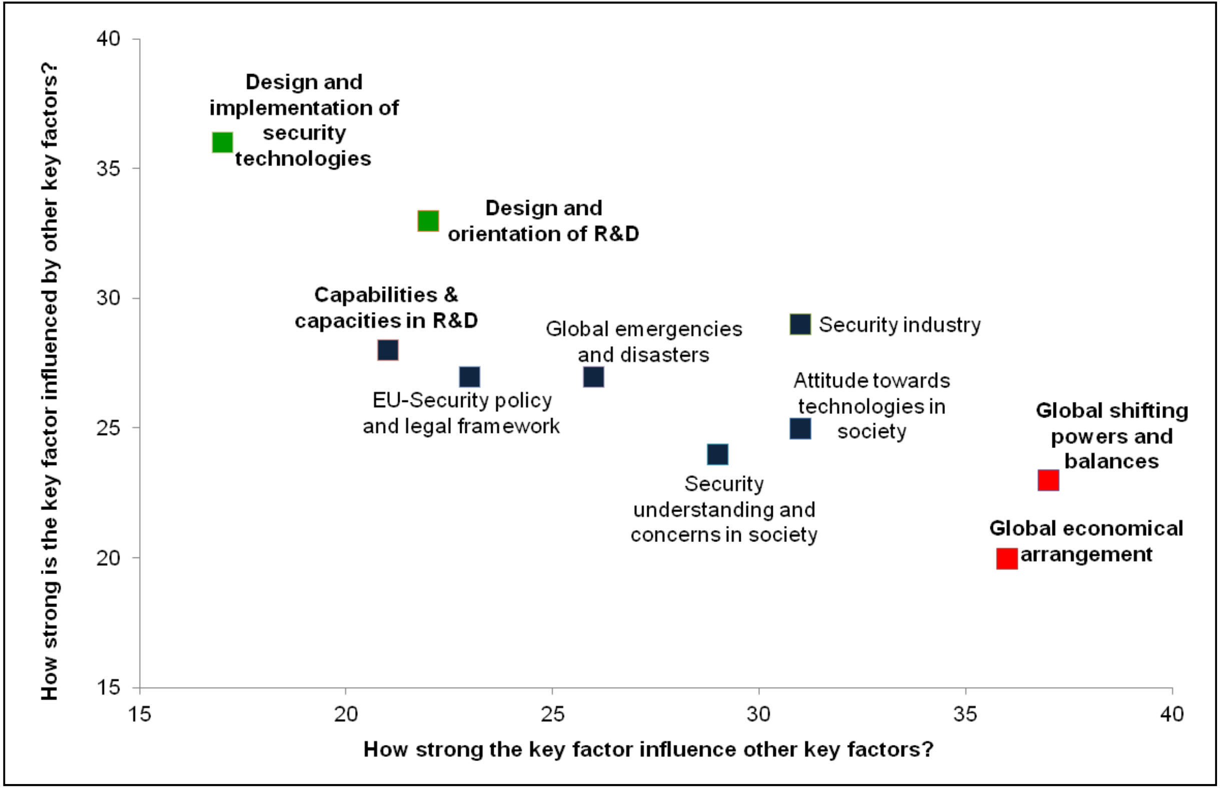
Table 4: Context factors and their passive and active influence levels

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

Source: ETTIS this report

The influence analysis of the context factors leads to general conclusions with regard to the importance of certain factors for the context scenarios: “Global shifting powers and balances” and “Global economical arrangement” have the strongest impact on the other factors. “Design and implementation of security technologies” and “Design and orientation of R&D” are the most passive factors; that´s means that they are the most influenced by other factors.

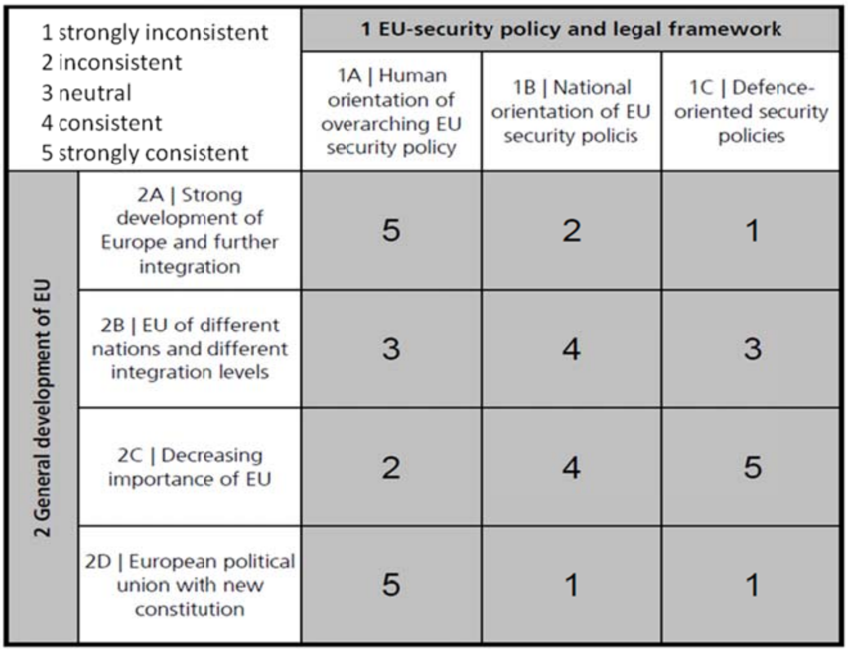
Figure 12: The most passive and active key factors – an extract



Source: ETTIS this report

Besides the influence analysis a further important step within the scenario analysis, a scenario building based on the ***consistency analysis***, was carried out. An important step within this process is generating a consistency matrix, where the fields contain consistency values between the future projections. The consistency matrix is used for generating bundles of future projections, which are the base for the scenario writing. For each pair of future projections of different key factors, WP4 team estimated, how compatible the two projections are to each other (see figure 10): 5 = strong consistency, 4 = consistency, 3 = no direct relationship, 2 = partial inconsistency and 1 = total inconsistency. This estimation sets a basis of which future projections should or shouldn´t appear in the same scenario.

Figure 13: Consistency matrix - future projections – an extract of two future projections



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

Source: ETTIS this report

Four context scenarios were developed by combining the future projections in a plausible way, the so called projection bundles. The most important criteria are: (i) firstly the internal consistency (within the future projections in a scenario), e.g. estimation about whether the projections might occur simultaneously in one scenario; (ii) secondly the external diversity (within different scenarios), e.g. selection of these scenarios which describe various future situations.

Five scenarios were presented in the consistency workshop, in order to gather the participants' opinion on the scenarios. The group discussions were oriented towards the following questions:

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

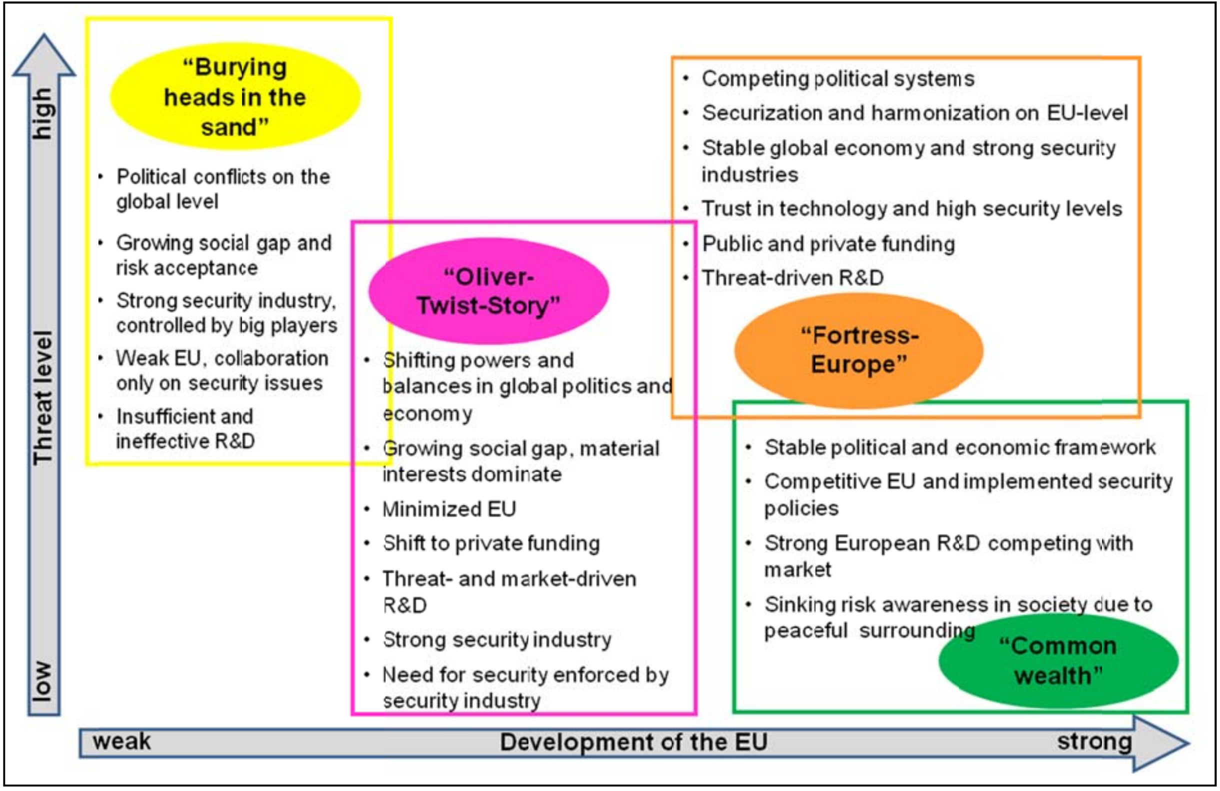
The discussion led to the adjustment of some future projections and helped clarify interdependencies and dynamics within the scenarios. As a result, the answers, opinions and recommendations are followed and addressed when editing the prepared scenario drafts. Taking in regard the workshop recommendations the context scenarios are finally reduced to four scenarios.

The four context scenarios are marked by the four different lines in figure 15. Each line is based on one bundle of future projections. Figure 14 shows an overview of the characteristics of each context scenario which resulted from the influence analysis:

- The dimension "development of the EU" is strongly correlated with the key factors "global economical arrangement" and "global shifting powers and balances", the most influent factors in the analysis.

- The dimension “threat level” refers to that, how many different threats or developments which might be threats are described by the future projections in each scenario (see also chapter 3.3, table 2).

Figure 14: Characteristics of the context scenarios in overview



“Burying heads in the sand”

- Political conflicts on the global level
- Growing social gap and risk acceptance
- Strong security industry, controlled by big players
- Weak EU, collaboration only on security issues
- Insufficient and ineffective R&D

“Oliver-Twist-Story”

- Shifting powers and balances in global politics and economy
- Growing social gap, material interests dominate
- Minimized EU
- Shift to private funding
- Threat- and market-driven R&D
- Strong security industry
- Need for security enforced by security industry

- Competing political systems
- Securization and harmonization on EU-level
- Stable global economy and strong security industries
- Trust in technology and high security levels
- Public and private funding
- Threat-driven R&D

“Fortress-Europe”

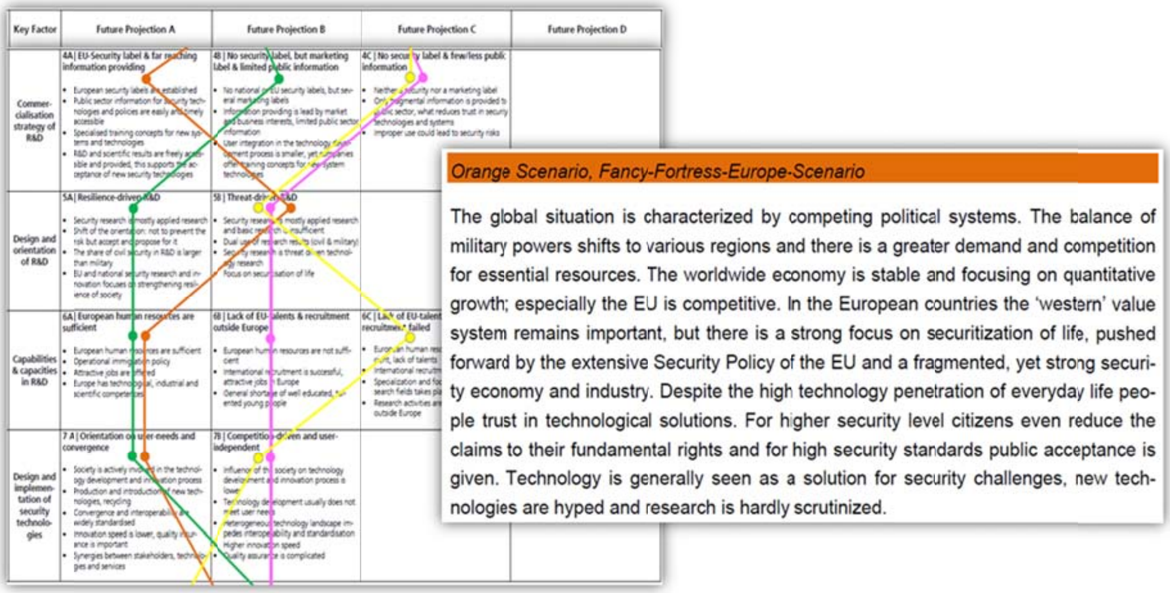
- Stable political and economic framework
- Competitive EU and implemented security policies
- Strong European R&D competing with market
- Sinking risk awareness in society due to peaceful surrounding

“Common wealth”

Source: ETTIS this report

These different bundles of the future projections were formulated to short scenario stories (1-2 pages) for the context scenarios as well as for the threat scenarios (see figure 15).

Figure 15: Formulation scenario stories based on the scenario paths – an example



Key Factor	Future Projection A	Future Projection B	Future Projection C	Future Projection D
Commer-cialisation strategy of R&D	4A| EU-Security label & far reaching information providing • European security labels are established • Public sector information for security technologies and policies are easily and timely accessible • Specialised training concepts for new systems and technologies • R&D and scientific results are freely accessible and provided, this supports the acceptance of new security technologies	4B | No security label, but marketing label & limited public information • No national or EU security labels, but several marketing labels • Information providing is lead by market and business interests, limited public sector information • User integration in the technology development process is smaller, yet companies offer training concepts for new system technologies	4C | No security label & few/less public information • Neither a security nor a marketing label • Only fragmental information is provided to public sector, what reduces trust in security technologies and systems • improper use could lead to security risks	
Design and orientation of R&D	5A| Resilience-driven R&D • Security research is mostly applied research • Shift of the orientation: not to prevent the risk but accept and propose for it • The share of civil security in R&D is larger than military • EU and national security research and innovation focuses on strengthening resilience of society	5B | Threat-driven R&D • Security research is mostly applied research and basic research is insufficient • Dual use of research results (civil & military) • Security research is threat driven technology research Focus on securitisation of life		
Capabilities & capacities in R&D	6A| European human resources are sufficient • European human resources are sufficient • Operational immigration policy • Attractive jobs are offered • Europe has technological, industrial and scientific competences	6B | Lack of EU-talents & recruitment outside Europe • European human resources are not sufficient • International recruitment is successful, attractive jobs in Europe • General shortage of well educated, talented young people	6C | Lack of EU-talent recruitment failed • European human res ment, lack of talents • International recruitm • Specialization and foc search fields takes pla • Research activities are outside Europe	
Design and implemen-tation of security technolo-gies	7 A | Orientation on user-needs and convergence • Society is actively involved in the technology development and innovation process • Production and introduction of new technologies, recycling • Convergence and interoperability are widely standardised • Innovation speed is lower, quality insurance is important • Synergies between stakeholders, technologies and services	7B | Competition-driven and user-independent • Influence of the society on technology development and innovation process is lower • Technology development usually does not meet user needs • Heterogeneous technology landscape impedes interoperability and standardisation Higher innovation speed • Quality assurance is complicated		

Orange Scenario, Fancy-Fortress-Europe-Scenario

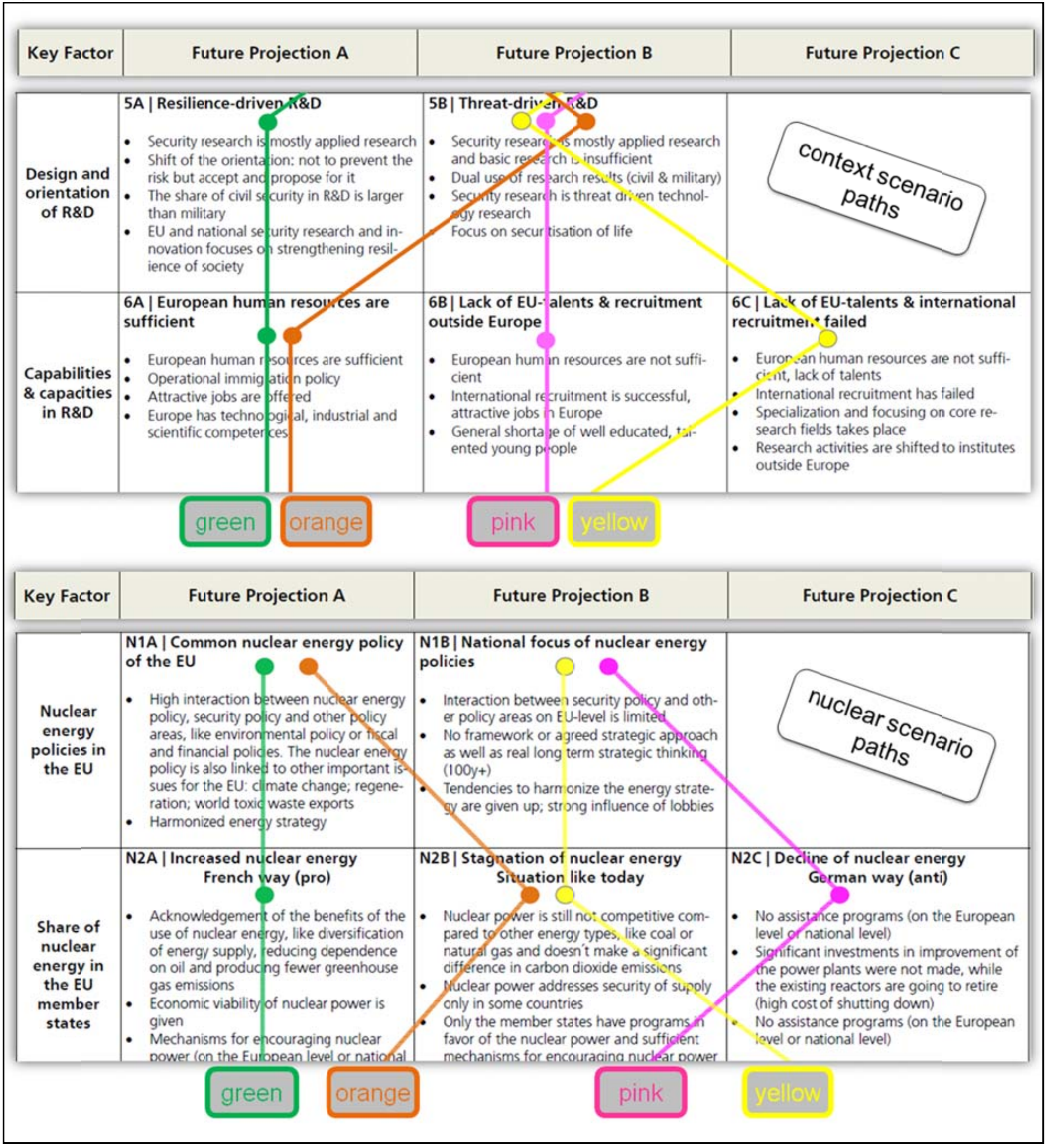
The global situation is characterized by competing political systems. The balance of military powers shifts to various regions and there is a greater demand and competition for essential resources. The worldwide economy is stable and focusing on quantitative growth; especially the EU is competitive.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

Source: ETTIS this report

4.3.3 *Threat scenarios*

Based on the context scenarios four threat scenarios for each domain (i.e., cyber infrastructure, nuclear and environment) were created using the same approach. The results are **four threat scenarios for each domain** which base on **four context scenarios** (see figure 16).

Figure 16: Exemplary four scenario paths within the domain nuclear



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

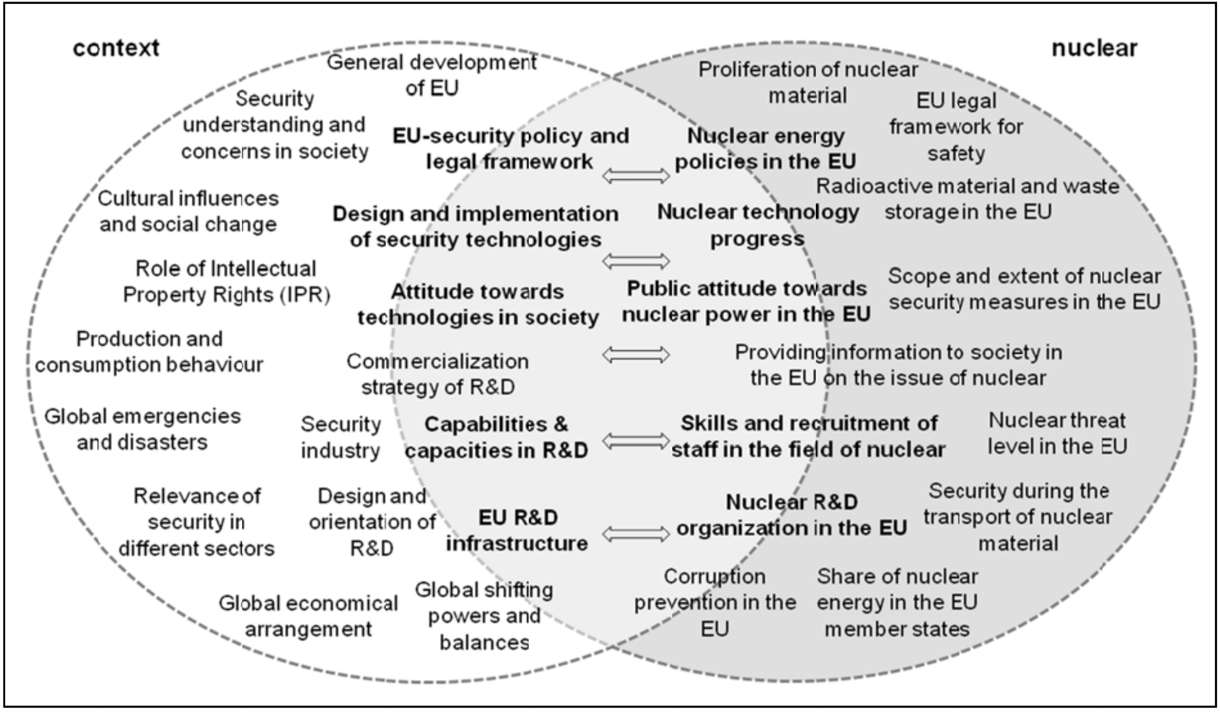
Key Factor	Future Projection A	Future Projection B	Future Projection C
Nuclear energy policies in the EU	**N1A | Common nuclear energy policy of the EU** • High interaction between nuclear energy policy, security policy and other policy areas, like environmental policy or fiscal and financial policies.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

Source: ETTIS this report

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

The underlying data for the scenario building, the key factors of the threat scenarios are presented in figure 17 (see nuclear as an example). The direct interfaces with the context key factors and the threat key factors are visible. They were used to link the context and the threat scenarios.

Figure 17: Linking context and environment



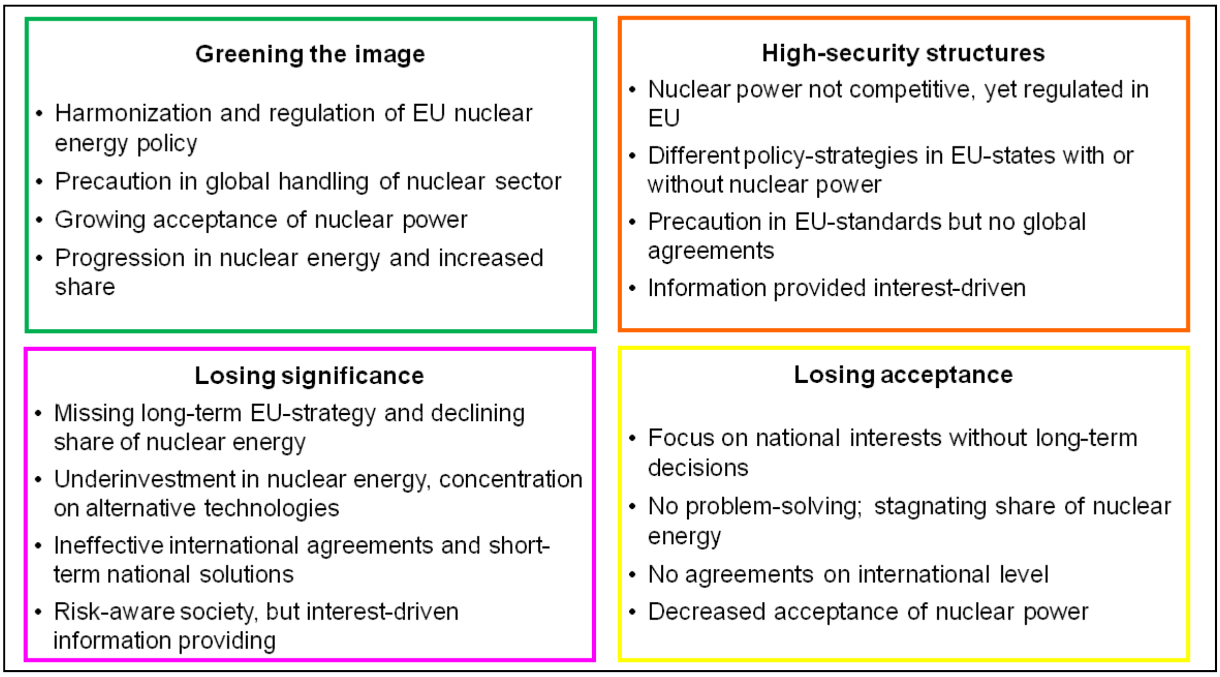
context
nuclear
General development of EU
Security understanding and concerns in society
EU-security policy and legal framework
Cultural influences and social change
Design and implementation of security technologies
Role of Intellectual Property Rights (IPR)
Attitude towards technologies in society
Production and consumption behaviour
Commercialization strategy of R&D
Global emergencies and disasters
Security industry
Capabilities & capacities in R&D
Relevance of security in different sectors
Design and orientation of R&D
EU R&D infrastructure
Global economical arrangement
Global shifting powers and balances
Proliferation of nuclear material
EU legal framework for safety
Nuclear energy policies in the EU
Radioactive material and waste storage in the EU
Nuclear technology progress
Public attitude towards nuclear power in the EU
Scope and extent of nuclear security measures in the EU
Providing information to society in the EU on the issue of nuclear
Skills and recruitment of staff in the field of nuclear
Nuclear threat level in the EU
Nuclear R&D organization in the EU
Security during the transport of nuclear material
Corruption prevention in the EU
Share of nuclear energy in the EU member states

Source: ETTIS this report

The consistency workshop was used to gather participants' opinion on how compatible the developments (described in different future projections) in each domain are with the context scenarios, as threat scenarios should be embedded in the different frameworks set by the context. Analogous to the discussion in case of the context scenarios also here the discussion led to the adjustment of some future projections and helped to clarify interdependencies and dynamics within the threat scenarios. Figure 18 shows an example of an overview of the characteristics of the threat scenarios. Short scenario stories (1-2 pages) were formulated for each threat scenario.

Figure 18: Characteristics of the nuclear scenarios[6]

[6] the link to the context scenarios is expressed by colours



Greening the image

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

High-security structures

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

Losing significance

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

Losing acceptance

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

Source: ETTIS this report

4.4 Critical review of scenario development in WP4

Based on the methodological discussion in chapter 4 and the description of the methodology used in ETTIS some findings should be pointed out and discussed in this chapter:

- Evaluation criteria for scenario development,
- Handling the different time horizons in the domains,
- Dynamics of scenarios.

4.4.1 Evaluation criteria for scenario development

The purpose of the scenario process is high relevant for choosing the appropriate approach. Besides the identification of societal security needs, the scenarios in ETTIS are used on the one hand to evaluate what kind of solutions could be suggested or should be developed to meet these needs; On the other hand to prioritise the solutions (Are they robust towards the different scenarios for one domain? Are they robust towards the different domains?) For this purpose it made sense to work with consistent scenarios describing plausible and different framework conditions for the solutions.

The description of the scenario approach in ETTIS (chapter 4) included already some reflections about the consistency analysis and further scenario validation criteria. The internal consistency (within one scenario) is an important attribute of any scenario as well as their external diversity (between different scenarios). Especially for complex problems with a large number of the key factors, the detailed analysis using the consistency matrix is recommended. Generating the bundles with future projections is based on one further important criterion, the diversity. This is important in particular for testing the robustness of solutions, which will be proposed according to the scenarios. This is the reason for not using probabilities in scenarios, which was a major discussion in the consistency analysis (chapter 4.1.1). However this aspect was discussed in ETTIS with the involved experts and within the consortium at different steps.

The plausibility of scenarios was supported by the influence analysis (see chapter 4.3.2) in which the interrelationships among the key factors were investigated. The analysis provided findings about which key factors might be the main driving forces in the scenarios and supported the development of an internal logic for each scenario.

A further criterion that was taken into account is the utility, which means that scenarios must meet a specified purpose. The purpose of scenario building in ETTIS is deriving societal needs and setting the different framework conditions for the analysis on how to handle the identified needs Thus the scenarios included a wide range of threats which are described by the future projections and have a high relevance for the identification of societal needs. As the validation workshop showed, in particular the intensity of the identified needs varies in the different scenarios.

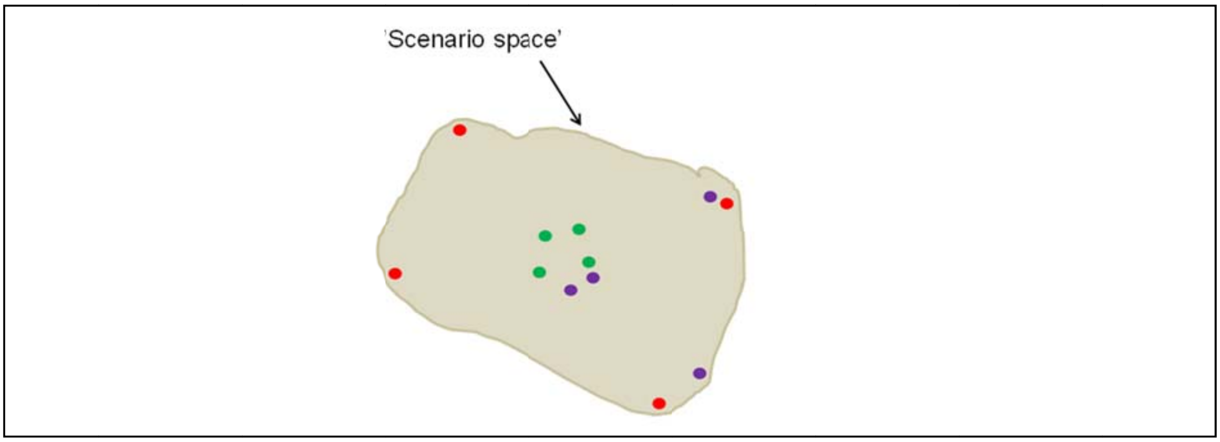
The intelligibility, which means that scenarios must be comprehensible and transparent, was supported by the documentation of each step of scenario development, e.g. the identification of the relevant aspects for the context and the domains; the expert´s identified priorities of these aspects and the selected key factors; the identified future projections both on a short and long term ; the results of the consistency analysis as a proven method for bundling the future projections within and across scenarios; the results of the influence analysis to set a solid basis for the scenario writing as well as the short scenario descriptions without considering preferences and values of the authors.

4.4.2 Diversity of scenarios

It has been suggested that in the development of scenarios it is necessary to strike a balance between plausibility and creation of new and challenging insights (Eriksson and Weber 2008; van der Heijden 2005). One of the key arguments for using scenarios (instead of e.g. prognoses/forecasts) in decision-making is that the future in general is very uncertain. One key strategy is then to search for robust strategies, i.e. strategies that work reasonable well across a wide range of future developments. In order to develop and assess the robustness of these strategies it is important that the scenarios are widely spread, i.e. that they are diverse (Kemp-Benedict, 2012). This means that the scenarios in a set should describe very different possible development paths of the future.

In general there are two ways in which a scenario set can fail to be widely spread: General conservatism, with all scenarios close together around some type of ‘business-as-usual’ future, or lack of balance in the sense that the set contains extreme hence challenging scenarios in some ‘directions’ and un-challenging ones in other (see schematic illustration in figure 19 below). The green points represent a conservative scenario set, the purple points represent an unbalanced set and the red points represent a broadly spanning set of scenarios.

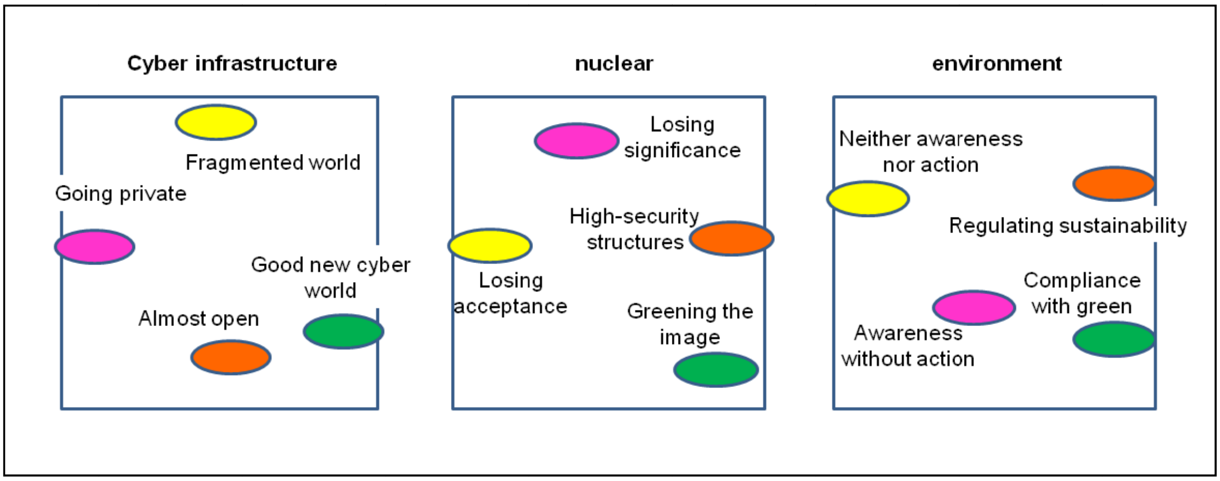
Figure 19: Schematic illustration of three archetypes of scenario sets



Source: ETTIS this report

Figure 19 shows, how spread are the developed threat scenarios. This chart is based on the mathematically calculated dissimilarities among the scenarios in each domain. The dissimilarity means the total number of different future projections and does not refer to a specific dimension, like in figure 20.

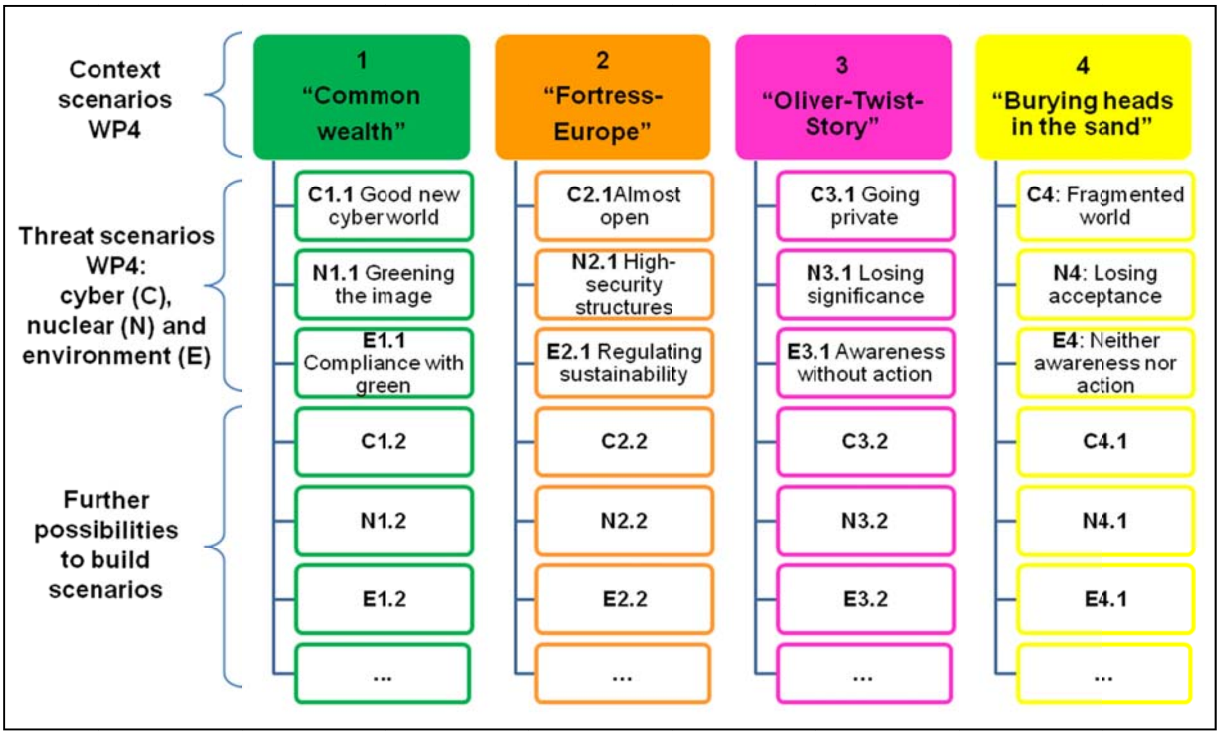
Figure 20: Diversity of threat scenarios (based on the context scenarios) in ETTIS



Source: ETTIS this report

One obvious way of assessing robustness of strategies is to assess the strategies over a larger set of scenarios. However, for analytic tractability it is necessary to limit their number (Bradfield et al. 2005). In this context there was a discussion on the required number of context and threat scenarios in ETTIS at the beginning of this project. Usually, for context scenarios, one work with something like 3 to 6 scenarios as illustrated in figure 20 above. Following this approach 3 to 4 scenarios for context and 3 to 4 scenarios for each domain were recommended (see D3.1). Moreover, it was noted that the number of threat scenario should be bigger than the number of context scenarios. Therefore 16 scenarios were developed in total: 4 context scenarios and 4 threat scenarios for each domain (see figure 20). This number of scenarios was not quite easy to handle by the experts in the validation workshop, above all in using the developed scenarios for the identification of societal security needs. Also in the consistency workshop five scenarios were proposed, four of them were selected by the consortium members as a basis for the development of threat scenarios. The spectrum of the different developments described in the scenarios is very broad. However from the theoretical point of view there is still a possibility to build further scenarios, based on the consistency analysis (see figure 21), if required by further project proceeding.

Figure 21: Increasing the number of threat scenarios



Source: ETTIS this report

In order to assess ETTIS methodology further, it would be valuable e to discuss the diversity and the number of scenarios in WP3.

4.4.3 Handling the different time horizons in the domains

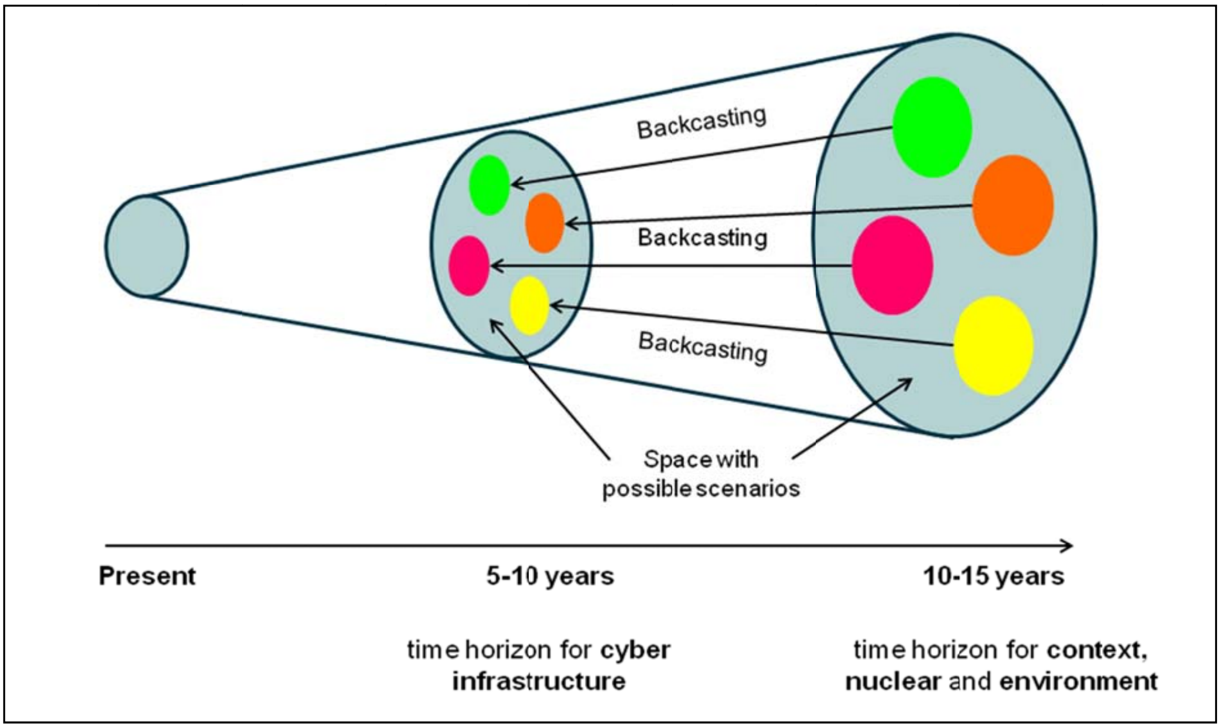
Different security domains require different time horizons. The considered time horizon in ETTIS differed across the different domains.: For the cyber domain a shorter time horizon has been set (5-10 years), opposed to the nuclear and environment domains where a longer time frame (10-15 years) was adopted. However, the scenarios for cyber infrastructure were implemented in the same context scenarios as the other domains (with the time frame 10-15 years, see figure 22).

This approach s is based on the assumption, that the in context scenario described developments (future projections) might also apply for a shorter time horizon. This assumption could be verified by a further investigation driven by the following questions:

- Which developments in the context scenarios are already realized in 5-10 years?
- For which future projections is an adjustment of the described development required?

This should be considered while including more domains with a different characteristic.

Figure 22: Time horizon in ETTIS


Backcasting
Backcasting
Backcasting
Space with possible scenarios
Present
5-10 years
10-15 years
time horizon for **cyber infrastructure**
time horizon for **context, nuclear** and **environment**

Source: ETTIS this report

Table 5 shows an example of future projections for the key factor "role of intellectual property rights". The future projection "national frameworks and strategic use of patents" (15C) could also apply to the time frame of 5 to 10 years, thus describing the forward projection of the "status quo". Conversely, the assumption "agreed upon EU patent" (15B) could be too "optimistic" and should be adjusted to the shorter time frame, e.g. "first discussion on an agreement upon EU patent". Alternative it could be exclude from the analysis.

Table 5: Context factors and their passive and active influence levels

	15 A | Open knowledge in EU	**15 B | Agreed upon EU patent**	**15 C | National frameworks & strategic use of patents**
Role of Intellectual Property Rights (IPR)	• Open knowledge - knowledge is seen as common property • Rare granting of exclusive patents • Open Source, Open Data and Crowd Sourcing • Working on common standards	• European harmonisation, Member states agreed upon EU patent; Actions depending on the sector (e.g. Software) • Protection of knowledge is important, confidential handling of knowledge	• No harmonisation on EU level; National laws dominate in the field of IPR • Multiple patent applications are necessary for protection; Strategic use of patents

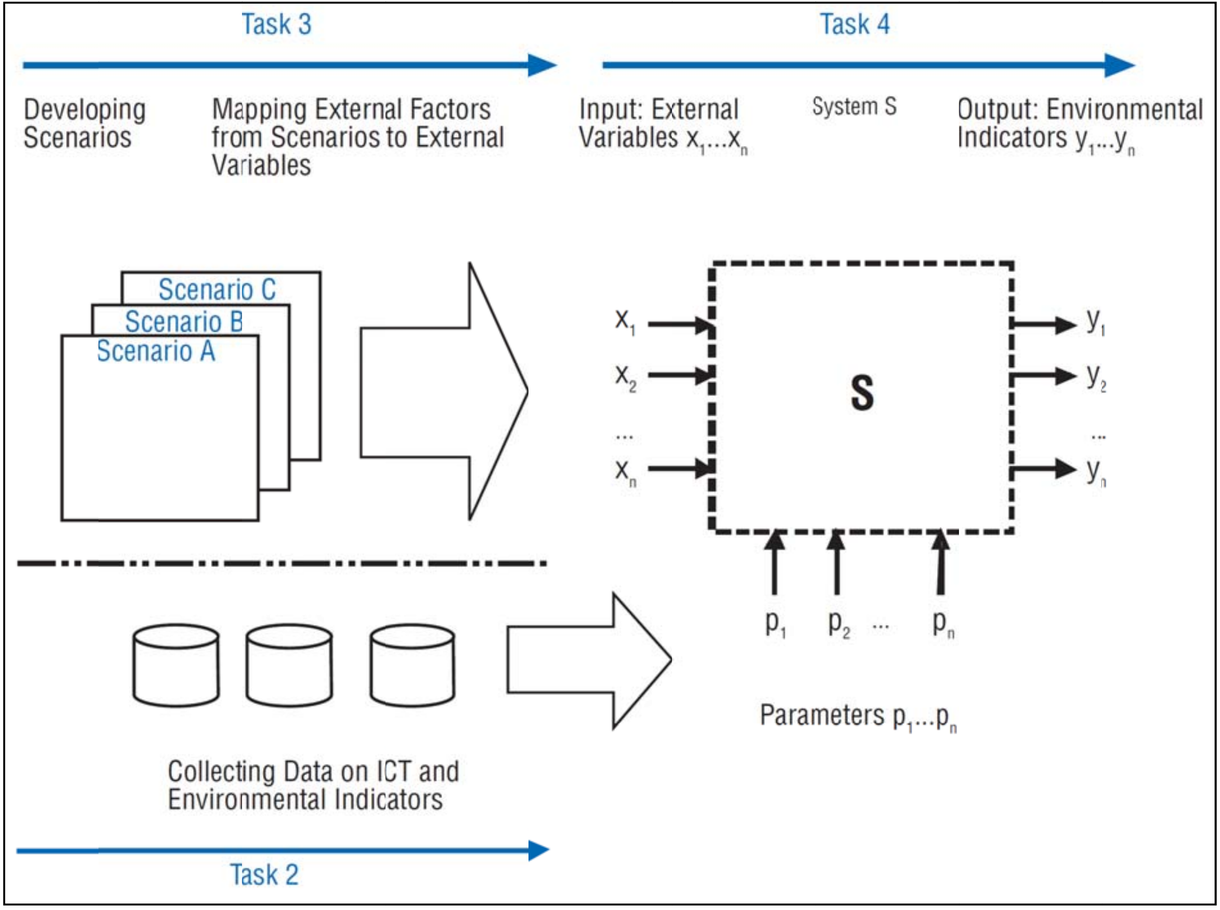
Source: ETTIS D.4.4 report

Dynamics of scenarios

One possible solution to capture the different time frames of the different domains could be the modelling of scenarios, which allows step-by-step-building of scenarios (see chapter 4.1.1). A typical procedure for the quantification of scenarios using system dynamics is presented by Erdmann (2004, see figure 23). He present also some lessons learned resulting from the practical experience with the quantification of scenarios by modelling (Kosko et al. 2008, p. 62):

- To quantify scenarios and translate them into models the consistency of the scenarios is required. Scenarios must be based on the same internal logic, such as the model otherwise the results are not interpretable. The consistency analysis is particularly suitable for this purpose.
- Fixed values for the quantification of future projections are not required, bandwidths are sufficient.
- The added value of modelling, also in comparison to qualitative methods of future research, is on the one hand quantitative results and n the other hand a systematic and transparent approach where the scenario and the modelling process supports the acceptance of the results.

Figure 23: Quantification of scenarios by system dynamics (hybrid scenarios)


Task 3
Task 4
Developing Scenarios
Mapping External Factors from Scenarios to External Variables
Input: External Variables $x_1 \ldots x_n$
System S
Output: Environmental Indicators $y_1 \ldots y_n$
Scenario C
Scenario B
Scenario A
x_1
x_2
...
x_n
S
y_1
y_2
...
y_n
p_1
p_2
...
p_n
Parameters $p_1 \ldots p_n$
Collecting Data on ICT and Environmental Indicators
Task 2

Source: Erdmann 2004, p. 20

The dynamics of scenarios in ETTIS was captured in two different ways:

- The influence analysis which identified the most influent key factors. Each future projection of these factors could be a starting point for a possible change of other developments (other future projections).
- The results of the influence analysis flowed into the scenario stories which follow this causal chain and in this way describe how events might unfold between now and the future in order to capture the dynamics of developments.

The influence analysis could build a bridge between the scenarios and the model, when it would be extended to the assumptions about the impact of the future projections. In the interaction matrix for each future projection it must be checked to which extent it is influenced by every other future projection and vice versa (see KSIM, chapter 4.1.1).

Furthermore, the future projections must be quantified to identify the variables for the model (see Table 6).

Table 6: Quantification of future projections – an example

Key factors	Examples of indicators
EU security R&D infrastructure	• RTD expenditure of the industry / RTD expenditure of the public sector / EU / nations • Number of similar themes in national and European research agendas • Duration of R&D cooperations • Number of research programs • …
Commercialization strategy of R&D	• Number of training concepts for new systems and technologies • Number of “open innovation” platforms • …
Design and orientation of R&D	• Number of security technologies • Number of technologies with dual use (civil and military) • Number of disaster and emergencies • …
Capabilities & capacities in R&D	• Supply-demand-balance of human resources in EU • Number of jobs in the security R&D • Development of wages and salaries in security R&D • …

Source: ETTIS this report

5 METHODS FOR NEED IDENTIFICATION

Based on the **threats scenarios** (see chapter 4.3.3) following a particular **context** (see chapter 4.3.2) as well as the **additional threats** (see chapter 3), a further analysis was carried out in order to identify **societal security needs**. The leading question of this investigation was: What happens when a threat occurs in the different scenarios? This analysis contains the following activities:

- Research based analysis of needs: Defining terms, structuring the existing classifications of needs, transfer of these results to the field of security, in particular to cyber infrastructure, nuclear and environment (input to WP3).

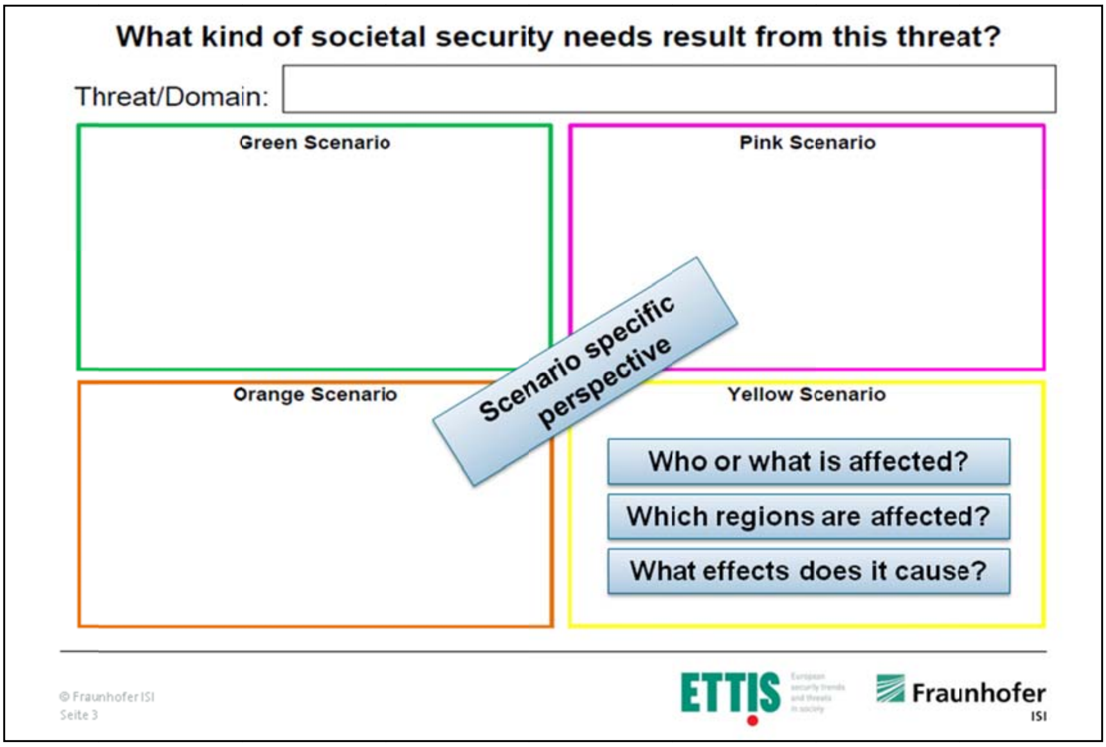
- Identification of societal security needs: Scenario validation workshop to derive needs based on the threats occurring in the different contexts, described by the context based threat scenarios.

The main source for the identification of societal security needs was the scenario validation workshop. In order to validate the outcome of the previous scenario development process, this workshop firstly contributed to the scenario discussion as well as to further identification and selection of threats for cyber infrastructure, nuclear and environment. Secondly, it provided additional crucial and solid groundwork for the identification of societal security needs by describing what happens when a threat occurs in different scenarios. The target group of the workshop was the user group encompassing the most relevant stakeholders from different security related organisations, civil society organisations, the public and researchers, high level policy-makers in the field of security as well as other stakeholders.

In general the scenario validation workshop included structured discussion with a selected group of experts, specifically in this case from the field of cyber infrastructure, nuclear and environment, to gain information about their views to security threats and needs referred to the scenarios as well as to the workshop's broader aims. The interaction among experts from different background is very important for obtaining several perspectives about the same topic. Therefore one workshop for all fields, cyber infrastructure, nuclear and environment was conducted. For this reason we also 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.

As a final result, the answers, opinions and recommendations were implemented in the further identification of societal needs. Taking in regard the workshop recommendations societal security needs were identified for alls scenarios as a final result of WP4 and a direct input to WP5 and WP6.

Figure 24: Identification of societal security needs



What kind of societal security needs result from this threat?

Threat/Domain:

Green Scenario

Pink Scenario

Orange Scenario

Yellow Scenario

Scenario specific perspective

Who or what is affected?

Which regions are affected?

What effects does it cause?

© Fraunhofer ISI
Seite 3

Source: ETTIS this report

Though the workshop was focused on validating the treats and their relations to different scenarios, one part of the work was dedicated to derive societal needs related to the identified threats. Each group was asked to name societal security needs which arise from the described threats. The initial discussion showed some difficulties related to this task:

- The first problem was that the **terming of societal needs respectively to societal security needs differed strongly** among the participants. Additionally the definition of societal needs as given by the consortia (see D3.1) was considered to be too abstract, though examples were presented.
- The underlying problem was twofold: One point is that **security needs, respectively societal needs, have different meanings** in the different groups, so results and conclusions might vary. The main difference was either on the focus on technical aspects, such as "traceability of actors" and "useable solutions" or more societal aspects such as "trust/confidence". Moreover, it was remarked that **security itself is a societal need**, where further detailing would lead to problems. This already indicates the second difficulty, the **differentiation between societal needs and resulting solutions**. In many cases the experts' suggestions combined needs and solutions like in the case of AI safeguards, where trust builds through regulation of the process (i.e. requirement of human action for critical decisions).
- All in all the discussion led to the questions **how societal security needs can be specified** and to what extend it is possible to separate needs and solutions/options during such a process of identification.

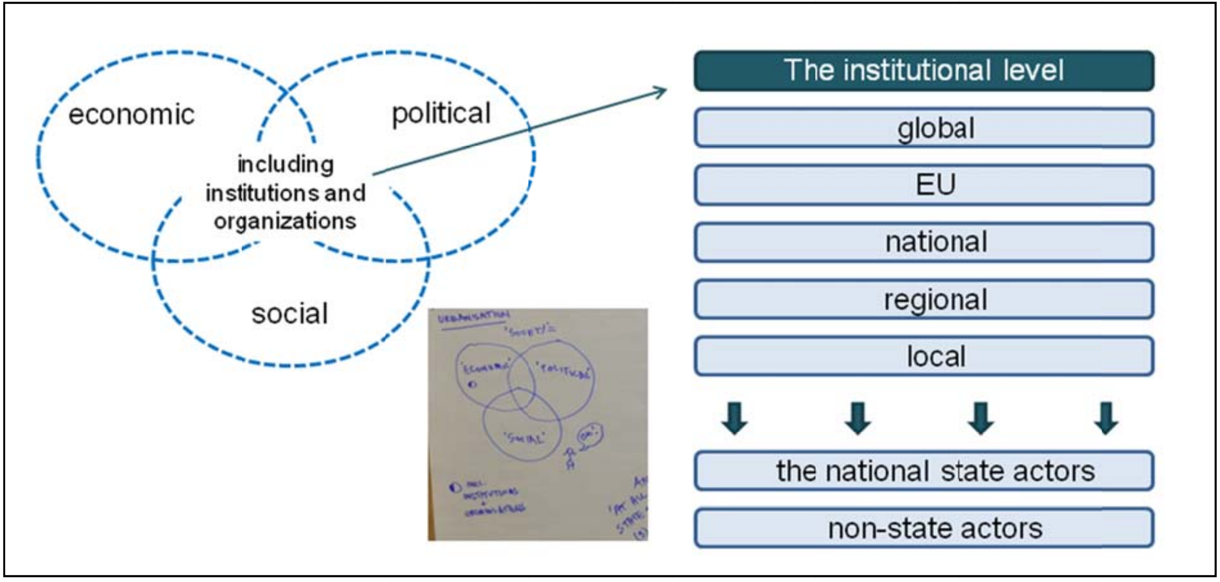
Based on this finding, the final process of identifying societal security needs focused on identifying overall societal needs in order to avoid the problems of differentiation described above. It was argued, that all threats, which are assigned to one of these threat sources, have the same effects on societal security needs. Further, it was argued that the same threats are possible in each of the four scenarios. The only difference is that some threats are more likely to happen and have a higher impact in some scenarios than in other ones. The societal security needs differ only slightly in the orange, the pink and the yellow scenario, whereas there are mostly other societal security needs in the green scenario.

Following insights and challenges with regard to the need identification should be pointed out:

- Deriving societal security needs was a challenge because of the blurry conceptual boundaries between needs and solutions and the practical difficulties of conveying the difference to others (interviews with stakeholders in the validation workshop). This could result from the specific nature of security being a need in itself. The more specific the description of the security need is, the more difficult the distinction between need and solution.. Thus, concrete needs mostly include solutions. Therefore, needs stay either at a more abstract level, describing issues like the need for protection, or easily end up at a level close to potential solutions, such as specific types of training measures or technical solutions. In principle, a higher level of description was desired in the analysis, but in some cases there were also more specific needs listed.
- There are also some other remarkable insights from the exercise. One relates to the challenge of ambiguity for which the question of identity in the internet is a good example. While in many cases like disproportion, but also in cases like data trails, the protection of anonymity would be seen as an advantage, many other cases show the need for clear identification such as vigilantism or cyber mobbing.
- Another challenge was handling the different perceptions of threats, i.e. the question if a threat is resolvable and how. The answer results in different level of impact in each scenario.
- Finally, there was the challenge to determine different needs for the different scenarios. In most cases, two, three or even four scenarios showed similar patterns for each domain. In those cases, it was hard to derive different needs. Only in some cases, it was clear that one or two scenarios strongly vary due to the different framework conditions in these scenarios. However, the impact differs between scenarios and is significantly higher or lower. Based on that assumption, the resulting needs will not vary so much across the scenarios. More differentiations would be possible if the likelihood of what is also taken into account. Therefore, different solutions should be proposed in different scenarios depending on the need intensity.
- There is a diversity of societal security needs across the domains, but there are still some overlaps:
    - Protection (e.g. of goods, immaterial goods, health, people),
    - Regulation (e.g. implementation, improvement),
    - Education, training (e.g. qualified workforce, educated society),
    - Information and transparency (e.g. about risks, measures, incidents)
    - International cooperation (e.g. regulation, agreements, enforcement),
    - Trust, reducing fear, safety culture and responsibility (e.g. trust in government, own responsibility)
    - Risk management (e.g. impact planning; simulation; modelling).
- It was challenging for the experts to handle the term "societal security needs". Identification of threats effects the following key questions: In which areas might the threat be relevant? For which institutions might this threat be relevant? For which

regions/ states might this threat be most relevant? What kind of influence might this threat have on these areas/ institutions/ regions? What might be potential risks?
As an example: There was a discussion about what is actually society and what are institutions (see figure 25).

Figure 25: Different aspect of society on institutional level[7]



Source: ETTIS this report

In addition to the discussions emerging from the scenario validation workshop, further activities to identify social security needs were part of WP4;: Firstly, the interviews with stakeholders in task 4.1 (see D4.5) and, secondly, the analysis of key works within security related future studies. This research-based analysis of needs contained i.e. defining terms, structuring the existing classifications of needs as well as the transfer of these results to the field of security, in particular to cyber infrastructure, nuclear and environment.

Furthermore an additional analysis of the literature related to the theory of needs (human needs) is under way in WP5 to extract and transfer additional theoretical insights to the project. There are important methodological insights expected from this analysis which will be transferred to WP3.

6 OPTIONS FOR SCENARIO DEVELOPMENT FROM WP5

As has been described in the report so far, scenarios played a crucial role in WP4. This is certainly true also in WP5. In this section a number of key observations regarding scenario development from WP5 perspective is drawn.

The aim of WP5 is twofold:

1. To identify emerging solutions for societal security needs, both of a technological and non-technological nature (technical artefacts and institutional structures);

[7] see dotted circles

2. To develop methodological components for the identification and assessment of solutions for societal security needs against the background of different scenarios.

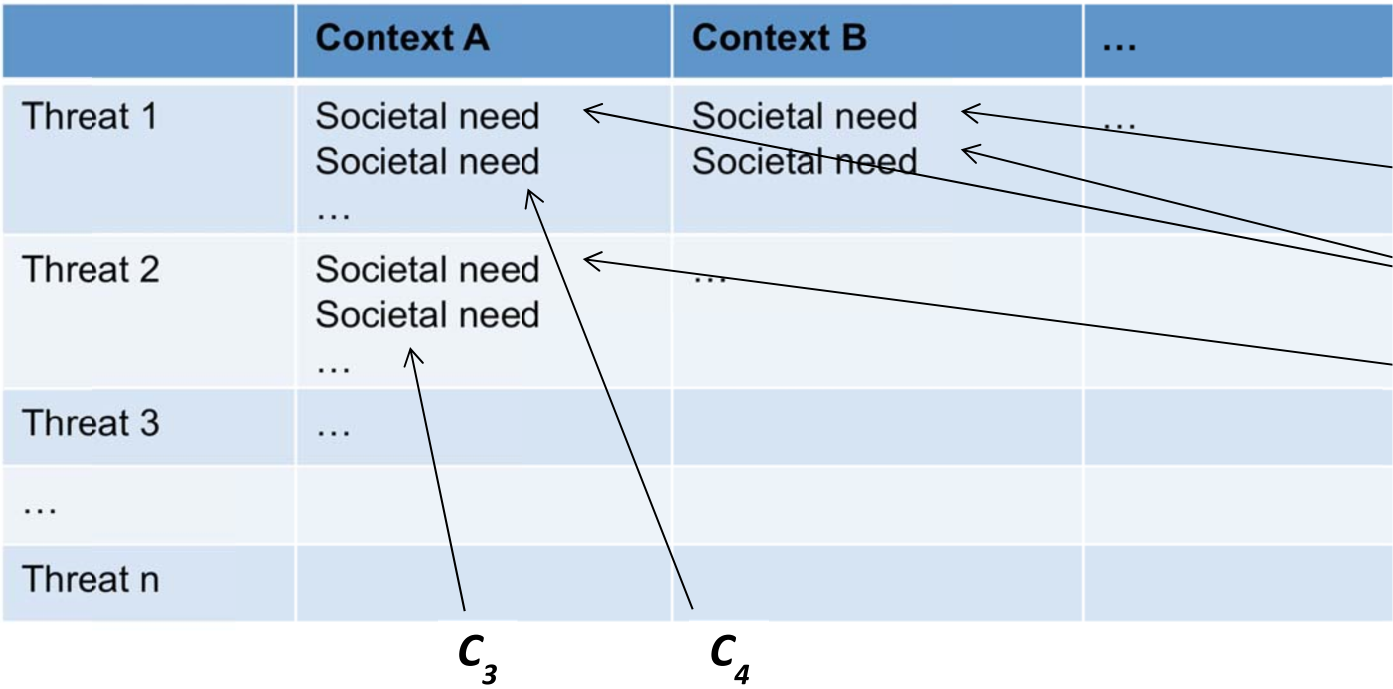
In short, the aim of WP5 is to *identify* and *assess* solutions for societal security needs. Scenarios are needed for both these tasks.

6.1 HOW TO ASSESS CURRENT AND FUTURE CAPABILITIES?

A solution for societal security needs is composed of *capabilities.* These capabilities can be of technical nature or institutional nature. Capabilities can be at our disposal, or not yet in place. The latter are capabilities that need to be developed and this is where the main issue of ETTIS, i.e. research and innovation prioritisation enters. In effect, what WP5 tries to address is to answer the question: Given a specific societal security need, now or in the future, what capabilities, at our disposal and not yet in place, do we need in order to meet this need? And what kind of research is needed to make the necessary capabilities available?

The starting point for the analysis in WP5 is the identified needs as indicated in table 3 on page 31 above. In this table, a capability addresses on or several societal needs in one and the same matrix element or in several matrix elements. The next stage in the analysis is to construct *portfolios* of capabilities, see illustration in figure 26 below.

Figure 26: ***Portfolios*** **of solutions**



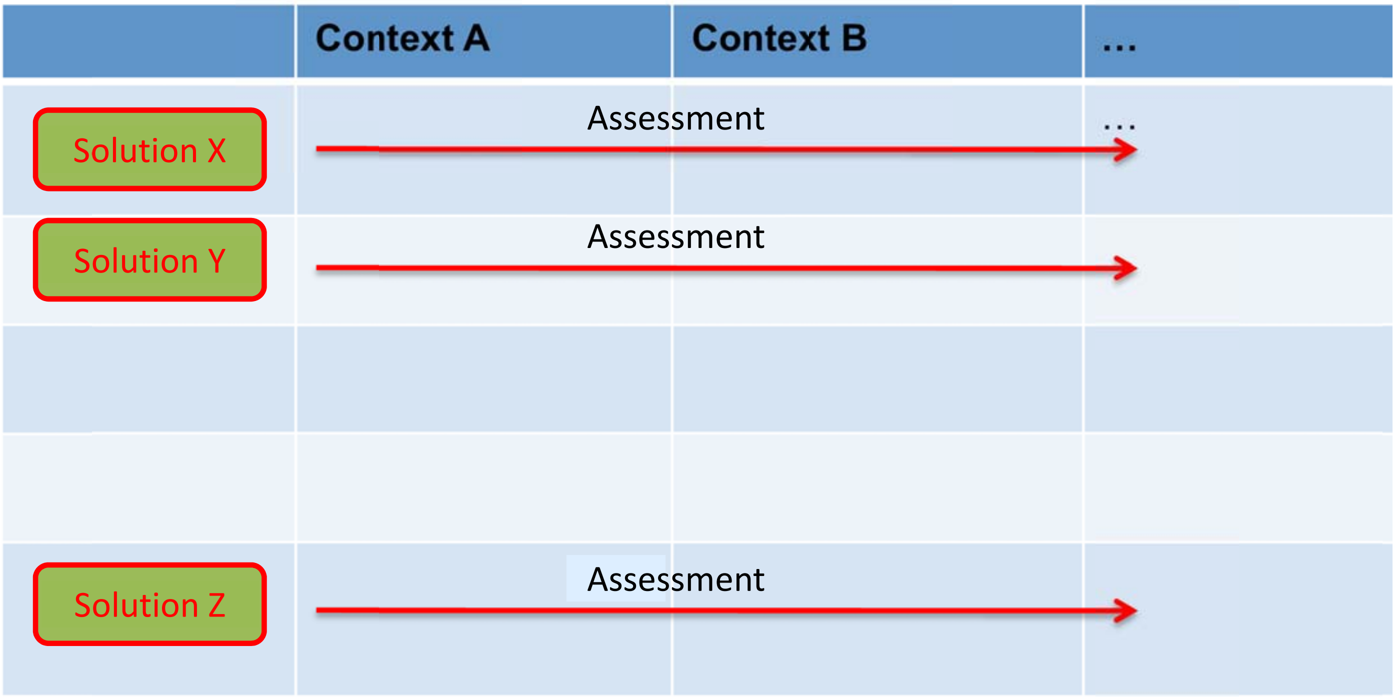
	Context A	Context B	…
Threat 1	Societal need Societal need …	Societal need Societal need	…
Threat 2	Societal need Societal need …	…	
Threat 3	…		
…			
Threat n			

Source: ETTIS this report

As is indicated in the figure, all capabilities except one (C_2) address only one societal need for one threat scenario in one context scenario. The solution constructed in this illustrative example – the portfolio consisting of the capabilities C_1 ,C_2 and C_3 – is capable of handling threat 1 in context B, and it contributes to the handling of threat 1 in context A and threat 2 in context A. It is important to underline that capabilities can be part of more than one portfolio, a feature not illustrated in the figure.

The assessment with regards to the different future societies, i.e. the context scenarios, will take place at the portfolio level; individual capabilities will not be assessed at this stage, see figure 27. However, since it is capabilities that give rise to research needs, individual capabilities will then be assessed. So, first we indentify robust portfolios of capabilities, i.e. portfolios that perform well over a range of context scenarios, and then these portfolios are analysed with regard to the capabilities that constitute them. In this stage of the analysis we foresee that network analysis could be used: each capability is a node and two capabilities are linked if they are part of any portfolio.

Figure 27: Assessment of solutions in face of ETTIS context scenarios



Source: ETTIS this report

As has been discussed above (section 4.4.3), different threat/challenge areas imply different time perspective in the scenarios used (eg. cyber vs. climate change), this is also the case for context scenarios as used in Figure 27. In any case, the solutions that are assessed in the matrix in Figure 27 contain information that should guide decision on research and innovation prioritisation *today and/or in a near future*. Hence, there is a time gap between the horizontal and vertical dimension in Figure 27.

In general this constitutes a serious problem, and one could debate how important a reduction of uncertainty is for decision-making in the context of research and innovation prioritization. While some consider accurate and reliable predictions to be an essential input in planning, others argue that one should rather look for alternative decision-making frameworks able to cope with deep uncertainty. And this is precisely what ETTIS attempts to do.

Naturally, different decision-making approaches are associated with these two positions. While the first view (sometimes called the ‘learn and predict then act’ strategy) can be related to an ‘optimum policy school’, the second position holds that one instead should seek for robust strategies, i.e. strategies that perform well even in the worst-case. However, instead of waiting for reliable predictions or seeking for a robust strategy, there is the alternative of applying a flexible strategy, i.e. a strategy that can be adjusted when new information becomes available. Other name for this is adaptive management in ecology (Walker et al. 2004) and real options theory in economics (Dixit and Pindyck 1994). The possibility to include "adaptive thinking" in research and innovation priority setting will be investigated in WP5 and WP6. This introduces a dynamical element into the ETTIS methodology.

6.2 HOW TO IDENTIFY SOLUTIONS

During the course of the ETTIS project a somewhat modified view on one of the basic assumptions underlying the project has emerged. When designing the project, threats identification was a corner stone of the approach taken. Although this is still a very important ingredient of ETTIS we do see a shift towards less focus on *identifying* threats and more focus on the aim, i.e. a more secure society. In other words, identifying sources of security is as important as identifying threats. This is also reflected in the shift of emphasis when comparing FP7's theme security to Horizon 2020's societal challenge Secure Societies – protecting freedom and security of Europe and its citizens. In effect, what we are witnessing is a shift from a threat-based research agenda into a resilience-based research agenda for tackling the societal challenge Secure Societies.

We think this shift has methodological consequences for ETTIS. One hypothesis is that, in a resilience-based approach to security, it will be less important to identify a *complete set of threats* (which is in practice always impossible, but still the ultimate goal) and more important to identify a *representative set of threats, against which key ingredients of resilience can be analysed and assessed.* With regard to capabilities the methodology need to be able to identify two types: i) defensive capabilities, i.e. capabilities that addresses a identified threat, and ii) resilience-enhancing capabilities, i.e. those capabilities that contribute to build a more resilient society. From a scenario methodological point of view this underlines the need to work with a diverse set of scenarios as discussed in section 4.4.2 above. This said, it will of course still be important to be able to identify threats in any effort to reach a more rational decision making process for research and innovation prioritization in the field of security.

In order to work with the task of finding a representative set of threats (or the more general term challenges) for a specific domain, it is important to work with threat/challenges scenarios on different systems levels and with differences with regard to the technology/institutional mix. A threat on high system level could be a scenario where the financial system is targeted, while a threat on low system level could be a new chemical drug targeted to teenagers. A threat with less technology/institutional mix could be a new explosives device, while new threat to personal integrity is most probably a mix between new technologies within ICT, new social habits and possible new regulations. The later will require an understanding of the evolving interaction between technologies and social change. In traditional sequential models of innovation, invention - ideas - precedes innovation, where innovation is when an artefact is introduced into social practice. In most case however – and to varying degree – such a model is too simple. Instead innovations evolve in a complex interplay between innovators and users. Perhaps the most prominent example of users taking part in the development of new technology is the invention of the World Wide Web. When Tim Berners-Lee wrote the first proposal on a system for information sharing at the European

Organization for Nuclear Research (CERN) he emphasized that it is impossible to predict how users will use the system.

In line with this reasoning , WP5 has identified a need to work with more detailed case studies within the three domains. For the cyber domain, the case study is concerned with what has been called “cyber situational awareness”. This is the cyber analogue of situational awareness in the physical space. Endsley (1995) has provide the perhaps most authoritative definition: “Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.”

A key technology in cyber situational awareness is information fusion. The idea is to fuse information from different sensors to get better information about an issue. What is meant by ”better” needs to be defined from case to case.

Cyber situational awareness underlines the need to shift the terminology from threat scenario to challenge scenarios: Cyber situational awareness could be a threat but it could also be a source of increased security. Hence, WP5 will build the case cyber situational awareness as a challenge scenario.

In order to develop the case study an internal ETTIS workshop was organised in Stockholm on 2013-08-21. The aim of the workshop was to start to construct a morphological field for cyber situational awareness. The idea is to construct a morphological field which can then be used for generating many challenge scenarios related to cyber situational awareness. In this way we intend to build a dynamical model that can be used for the identification of needs and solutions and assessed across context scenarios. The workshop identified 15 key factors and for some of those factors different future projections were constructed. Examples of key factors include “Actor”, “Cyber situational tasks” and “Legal framework”. For the first of these key factors identified future projections were “NGO”, “Criminal organisation”, “Individual” and “Lobby organisation”. For the complete list of key factors and future projections, see Appendix.

In two brainstorming sessions we generated proposed variables and variable states. States were constructed only for a few selected variables.

Table 7: Example of a morphological field in CSA

Variable Nr.	Variable Name	possible states
1	Actor	1A: NGO
		1B: Lobby organization
		1C: Civil society organization
		1D: Individual
		1E: International governmental organisations (eg. EU, Nato, UN,..)
		1F: Activists
		1G: Governmental organisations
		1H: Criminal organisations
		1I: States
		1J: Terrorist organisations
		1K: Corporations

		… and combinations of these
2	CSA tasks	2A: Early warning of interesting events
		2B: Real time monitoring
		Intelligence preparation of the battlefield
		2D: Identifying long-term trends
		2E: Tracing the impact of your actions
		2F: Credibility and reliability of information
		2G: Identify typical patterns
		2H: Exposed deception
		2I: Targeted information sharing
3	Legal framework	3A: Weak protection of the public and of private integrity
		3B: Weak protection of the public and strong protection of private integrity
		3C: Strong protection of the public and weak protection of private integrity
		3D: Strong protection of the public and of private integrity

Source: ETTIS this report

In addition to these three variables, the following variables were generated.

Table 8: Additional possible variables for the CSA morphological field

Variable no.	Variable name
4	CSA system
6	Infrastructure
7	Access to information
8.	Credibility and reliability of information provider
9.	Reference information
10.	Ownership of data
11.	The other guy intent
12.	The other guy – capabilities
13.	People's cyber habits
14.	Companies' cyber habits
15.	Processing and interpretation of information

Source: ETTIS this report

This information is currently the subject for further analysis within WP5. The aim is to be able to construct a number of challenge scenarios from the morphological field in accordance with the requirements discuss above. Other cases will also be developed within WP5 in order to further advance the methodology.

7 METHODOLOGICAL DISCUSSION POINTS

After more than 1 1/2 year of research in ETTIS some discussion points arise. Methodical developments are in the centre of ETTIS research. However to be useful the methods developed in ETTIS should have a practical value, they should be relevant to end users and reliable in their application to practical problems in research and innovation planning/prioritisation.

Even if the comments to quality of our research methods were discussed in each methodical chapter in this report, there are some discussion points, relevant to all work packages, which should be discussed in the following.

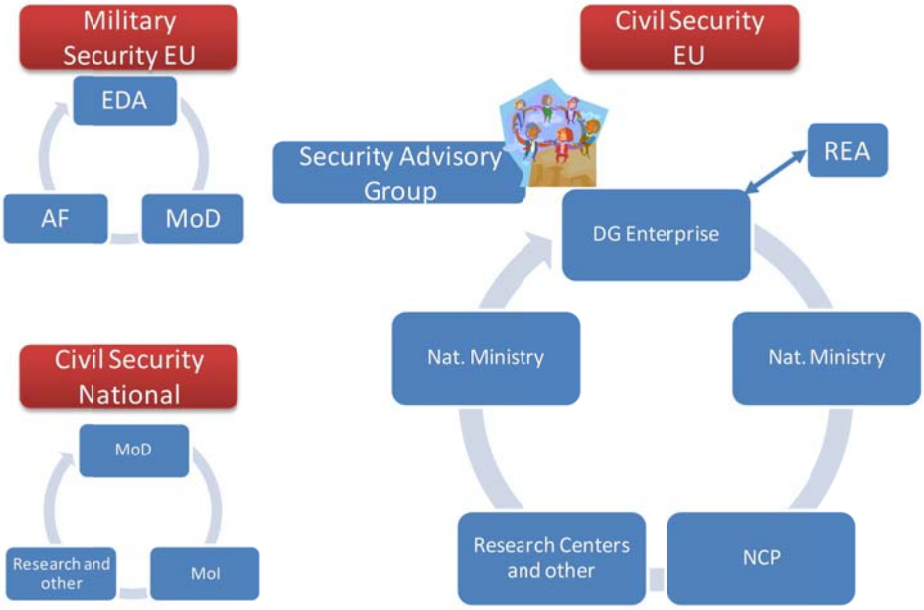
Scenarios are a core activity in ETTIS. They are used in WP4 and WP5 and they will be used in WP6. There is a huge amount of different techniques to develop and use scenarios. Often the decision to use one or another technique is not self-explaining and should be discussed in relation the purpose of the research objectives. This was the reason to include the first results from WP5 into this report. Comparing the threat scenarios from WP4 and the morphological fields for specific threats as utilised in WP5, it becomes obvious, that the level of abstraction, the descriptive items and the content are different. This means, that there might be a need for some adjustments to the work plan in ETTIS.

In addition to this, the threat identification methods delivered a wide range of different weak signals for threats, options, needs, wild cards and disruptive events. By now, this is widely unused in the project and there might be some opportunity to include this in the ETTIS work. From a substance point of view, one possible strategy would be to use this raw data as an input to the task of identifying the capabilities that build up solutions in WP5. This could be used as a "seed set" of capabilities for the Delphi study (Task 5.3). In this way, the pre-identified capabilities could act as inspiration of the respondents when they are asked to generate further capabilities as a basis for the construction of portfolios, i.e. solutions to societal security needs. Of course, this implies a considerable effort of back-office work in order to interpret the automatically generated output since the raw date needs human reasoning and interpretation (see further chapter 3.2.3). In most case this work includes the necessary translation of a threat, a need or an option into capabilities. This is far from a non-trivial task.

ETTIS has a commitment to usability for end user. From a practical point of view, ETTIS will produce a list of research topics for a future security research agenda (either Horizon 2020 or national) to demonstrate that the methods developed in ETTIS can contribute substantial inputs to long term research and innovation management. Therefore it is a good time to be very specific in the processes of how the research results fit into the work of e.g. policy makers; first aiders, strategic planner, etc. How can we make sure, that they will have interests in results and that they will get informed about the existence of these results?

The following figure shows a broad overview of who is formally involved in national and EU security research coordination and agenda setting. However, reality is more complex than these pictures suggest, with several informal processes of sense-making and lobbying superposing the formal processes. The WP6 team is right now working on a more in detail process description of agenda setting activities in the security domain.

Figure 28: Agenda setting in security research



Source: AIT

In addition the existing process of agenda setting in security research, new processes are discussed in the context of the European Forum on Forward Looking Activities (EFFLA).

According to the EC homepage[8], "the Forum brings together a set of high-level experts and decision makers from Academia, Industry, Government, European and International Organisations, NGOs, as well as think tanks, with very diverse profiles, able to mobilise the best available expertise and interact with key networks. EFFLA is consists of 15 full members."

The EFFLA "model" for future strategic decision processes, is based on four steps of strategic intelligence, sense-making, decision-making and implementation. In each of the phases, different actors are involved, either formally or informally. ETTIS methods can support such strategic foresight activities at different levels, if the methods are consistent to the level of generalisation.

The results from ETTIS are applicable for end users if they are relevant and reliable. Thus we should assess our methods in terms of whether they deliver relevant and reliable inputs to decision-making by these end-users, in addition to scientific validity and credibility.

Our selection of topics (environment, nuclear, cyber) was initially influenced by the EC, but later on also supported by our statistical indicators of the web crawling activities, as described in D4.4 (the more web links, the higher is the popularity of the topic). As a result from the web crawling statistics, it turned out to be no constraint to search for threats in the three domains, if these domains follow a broad definition. In particular the cyber domain and the environment domain are involved in almost all new future threats. All three domains cover almost all future threats, but it is not very helpful to discuss, whether a threat like collapse of

[8] http://ec.europa.eu/research/era/effla_en.htm

the waste in the stationary orbit is a cyber threat (it will cause the breakdown of the communication worldwide, or an environmental threat, because it is caused by space waste). So, in reference to the original goal of the scanning activity- to start with no domain exclusion- it is not much more restrictive to search in these domains, as these three domains are not restrictive. However in a real world application of the ETTIS scanning methods, we should usually start to operate without domain restriction.

Given the focus of WP5 on cyber situational awareness, climate induced migration and a nuclear threat; this indeed will lead us into a more restrictive analysis, which should be considered in the WP6 methodical discussion.

In WP4, we identified different types of threats. It is probably worthwhile to go into a more in detail analysis of these threats to find more "general" ways of protection. Dealing with different types of threats is common in national risk maps. A comparison of the threats from ETTIS, with the threats, already mentioned in national risk maps could give some insights into which threats are not well known in EU countries. In addition this would provide the opportunity to be more consistent with these risk maps and thus be more effective in communication of new threats.

While working on WP4 there were different discussions about the time frame of scenarios and the time frame of ETTIS. On the one hand timing is very important for strategic long term planners, as they need to build up future capabilities right in time. On the other hand it is a resilient strategy to address unknown time frames, by leaving out timing.

8 CONCLUSIONS AND PROPOSED ADAPTIONS TO THE ETTIS METHODICAL CONCEPT

This report aimed at summarising and assessing methodological insights from WP4, especially concerning scenario development, scenario utilisation and weak signal scanning. In addition to this, the report started a discussion about the contribution of WP 4 research in the overarching ETTIS research framework. After presenting the methodical work of WP 4 it becomes clear, that part of the ETTIS goals have been reached (marked in grey in the following list), while others are still open (marked in blue in the following list).

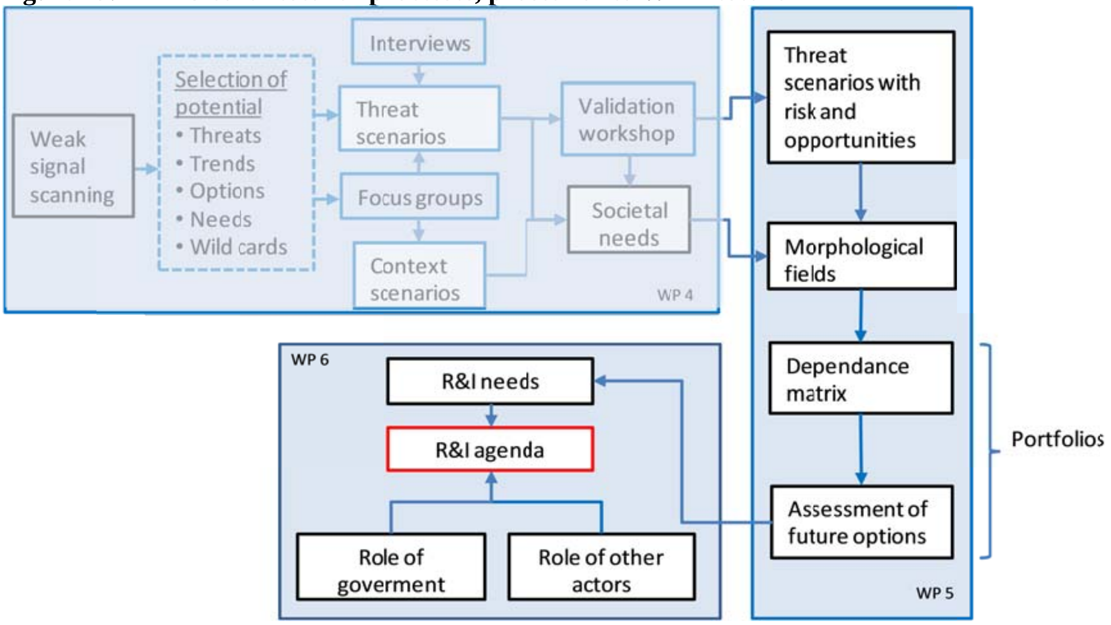
As mentioned at the beginning of this report, the aims of the ETTIS project are

1. *"to identify, understand and assess in a scenarios framework future threats, needs and opportunities for societal security,*
2. *to develop and test a methodological approach and model for a revolving process of security research priority setting,*
3. *to derive research priorities geared towards the needs of user organisations, as well as rationales and options for policy intervention, and*
4. *to help increase awareness of and attention to security research results, and contribute to overcoming barriers by advancing and testing a range of intelligence tools and techniques.*"[9]

[9] ETTIS B-Form

The final purpose of ETTIS is to contribute to a new security research agenda, either on a national level or on EU level. The following figure shows the core research process of ETTIS from a timing perspective. WP 4 is nearly finished, WP 5 is running and WP 6 started already.

Figure 29: ETTIS core research processes, prosterior to WP4 research



Source: ETTIS this report

From a theoretical point of view the process in figure 29 is simple and clear. From weak signals, we come to new threats and new social needs in WP 4. From existing solutions and capabilities we identify future capabilities and research needs to support long term strategic planning and contribute to a new research agenda.

From a practical point of view the question arises on how to produce a portfolio of research topics in WP 5. Given the fact, that it was difficult to identify new societal needs (societal needs are not as consistent as expected), it might be difficult to identify existing capabilities, not to speak of future capabilities and associated research needs. The challenge for WP 5 now consists of specifying solutions, capabilities and research needs and for WP 6 to derive research priorities from these capabilities and research needs.

Nevertheless, it was possible in WP 4 to identify:

- weak signals (which point to future threats, opportunities, needs or wild cards)
- trends
- wild cards
- disruptiv events
- some new threats and opportunities
- and societal security needs.

In addition and partly based on these results WP4 produced diverse and consistent context scenarios. The so-called threat scenarios in WP 4 are not at the level of single threats, but more abstract and focusing mainly on threat domains. We did not produce any information about the time horizon and impact of threats in WP 4, as this is usually not known or not possible to create due to epistemic limits.

WP 5 will produce morphological fields for the three use cases: cyber situational awareness, climate induced migration and at nuclear case, which still needs to be defined in more detail. In addition, as described in chapter 6, WP 5 will produce a methodology for assessment of existing and future solutions as a basis for the prioritisation of future research needs in the three aforementioned cases.

A first methodical concept of WP 6 point to the direction, that the context scenarios from WP 4 are suitable for war gaming. In WP 6 two different workshops are planned. WS I aims at making interests and value judgments explicit. For instance, security needs, budgetary constraints and industrial interests do not necessarily cohere, but need to be balanced to achieve an acceptable outcome. WS II will specify priorities and formulate the trade-offs resulting from these choices. Both topics are suitable for group discussions, having in mind the concept of adaptive planning.

For this process it would be necessary to have a list of threat topics, societal security needs and possible research topics. A critical point for this concept is that the level of abstraction and the level of detail need to fit the intended outcome.

From a methodological point of view the following conclusions regarding the continuation of ETTIS can be drawn:

1. Scenarios were foreseen to play a key role throughout the whole project. The experience from the work in WP4 is that this is still true: Scenarios are a key methodological constituent of the ETTIS methodology for research and innovation prioritisation.

2. However, WP 4 has created a "scenario jungle" that needs to be tamed. There are many different types of scenarios – broad context scenarios, more specific context based threat scenarios, and detailed descriptions of threats. Additional scenarios are foreseen in WP 5. It is crucial for ETTIS that the appropriate level of abstraction is applied for each scenario type. It is fair to say that this task has not and could not been fulfilled in a single report. It needs further discussion between all partners in WP 5 and WP 6 and should probably be discussed in the whole consortium.

3. The work in WP4 concerning scenario development included quantitative techniques, especially consistency analysis. Another technique that was discussion in this report is diversity analysis. Hitherto in the project, the methodological development with regard to quantitative scenario development has been very limited, the work has rather focus on utilising well established techniques for scenario development. However, this report has indentified possible such development path, e.g. the combination of consistency and diversity analysis for scenario development. Such methodological development is currently elaborated in WP5.

4. Another issue regarding scenario development is the handling of different time perspectives. This aspect of scenario development was highlighted by the huge difference in inertia between the domains cyber and nuclear. This issue was discussed from a methodological point of view, but here further research needs to be done.

5. During the course of the work in WP4 we have witnessed a tendency of moving from a threat based perspective on security research to a more ‘resilience’ based approach, in Horizon 2020. This is no strict dichotomy; it is rather a shift in emphasis. This shift has methodological implications yet to be explored.

6. This report has laid the ground for the work of identifying and assessing solutions to societal security needs, i.e. the work of WP5. The work in WP4 has been heavy towards substance, with the delivery of a huge amount of substantive information. In order to advance the methodological development in ETTIS further, WP5 will show a different balance between substance and method.

9 REFERENCES

Amer, Muhammad; Daim, T.U.; Jetter, Antonie: A review of scenario planning, Futures, 2012, Elsevier GmbH, München

Bentham, J.B.: Scenarios: An Explorer's Guide, Exploring the Future, 2008, Shell International BV, The Hague

Bowman, Gary; MacKay, R.B.; Masrani, Swapnesh; McKiernan, Peter: Storytelling and the scenario process: Understanding success and failure, Technological Forecasting & Social Change, 2012, Elsevier GmbH, München

Brabandere, Luc de; Iny, Alan: Scenarios and creativity: Thinking in new boxes, Technological Forecasting & Social Change, 2010, Elsevier GmbH, München

Bradfield, R., Wright, G., Burt, G., Cairns, G., van der Heijden, K., 2005. The origins and evolution of scenario techniques in long range business planning. Futures 37, 795–812.

Brauers, Jutta; Weber, Martin: Szenarioanalyse als Hilfsmittel der strategischen Planung: Methodenver-gleich und Darstellung einer neuen Methode, in: ZfB, 56 Jg. 1986, Heft 7, S. 631-650.

Brunner, Anne: Kreativer denken, Konzepte und Methoden von A-Z, 2008, Oldenbourg Wissenschaftsverlag GmbH, München

Dönitz, Ewa,J.: Effizientere Szenariotechnik durch teilautomatische Generierung von Konsistenzmatrizen, Forschungs-/Entwicklungs-/Innovations- Management, Gabler GWV Fachverlage GmbH, Wiesbaden, 2009

Durance, Philippe; Godet, Michael: Scenario building: Use and abuses, Technological Forecasting & Social Change, 2010, Elsevier GmbH, München

Eriksson, E.A., Weber, K.M., 2008. Adaptive foresight. Navigating the complex landscape of policy strategies. Technological Forecasting and Social Change 75, 462-482.

Fink, Alexander; Schlake, Oliver; Siebe, Andreas: Szenariogestützte Strategieentwicklung, in: Zeitschrift für Planung, 2000a, Band 11, S. 41-59.

Gausemeier, Jürgen; Fink, Alexander; Schlake, Oliver: Szenario-Management. Planen und führen mit Szenarien. München, Wien: Hanser 1995.

Geschka, Horst; Paul, Ingeborg; Winckler-Ruß, Barbara: Szenarien – ein Instrument der Unternehmens-planung, in: Zerres, Michael P., Zerres, Ingrid (Hrsg.): Unternehmensplanung – Erfahrungsberichte aus der Praxis. Frankfurt am Main: Frankfurter Allgemeine Zeitung 1997, S. 55-68.

Geschka, Horst; Reibnitz, Ute v.: Die Szenario-Technik – ein Instrument der Zukunftsanalyse und der strategischen Planung, in: Töpfer, Armin; Afhelt, Heik (Hrsg.): Praxis der strategischen Unternehmens-planung. Frankfurt am Main: Metzner 1983, S. 125-170.

Gierl, Heribert: Eine neue Methode der Szenario-Analyse auf der Grundlagen von Cross-Impact-Daten, in: Zeitschrift für Planung, 2000, Band 11, S. 61-85.

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

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

Groves, D.G., Lempert, R.J., 2007. A new analytic method for finding policy-relevant scenarios. Global Environmental Change 17, 73-85.

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

Hofmeister, Peter: Evolutionäre Szenarien. Dynamische Konstruktion alternativer Zukunftsbilder mit unscharfen Regelbasen. Hamburg: Kovac 2000.

Kane, J.: Water Resources Research, Volume 9, Issue 1, S. 65-79, 1973

Kemp-Benedict, E. 2012. Telling better stories: Strengthening the story in story and simulations. Environmental Research Letters 4, 041004.

Kosow, Hannah; Gaßner, Robert, Erdmann, Lorenz; Luber, B.J.: Methoden der Zukunfts- und Szenarioanalyse Überblick, bewertung und Auswahlkriterien, WerkstattBericht Nr. 103, Institut für Zukunftsstudien und Technologiebewertung, 2008, IZT, Berlin

Lempert, R.J., Groves, D.G., Popper, S.C., 2006. A genral, analytic method for generating robust strategies and narrative storylines. Management Science 52, 514-528.

Lindgren, Mats; Bandhold, Hans: Scenario Planning. The link between future and strategy. Great Britain: Creative Print & Design 2003.

Mißler-Behr, Magdalena: Bewertungsprinzipien für Zukunftsbilder: Ein Überblick, in: Gaul, Wolfgang; Schader, Martin (Hrsg.): Mathematische Methoden der Wirtschaftswissenschaften: Festschrift für Otto Opitz. Heidelberg: Physica 1999, S. 318-327.

Mißler-Behr, Magdalena: Methoden der Szenarioanalyse. Wiesbaden: Deutscher Universitäts-Verlag 1993.

Mißler-Behr, Magdalena: Methoden der Szenario-Erstellung, in: Gausemeier, Jörgen (Hrsg.): Die Szenario-Technik – Werkzeug für den Umgang mit einer multiplen Zukunft: Paderborner Szenario-Workshop am 14. November 1995, 1. Auflage. Paderborn: HNI-Verlagsschriftenreihe 1995a, S. 43-62.

Möhrle, Martin G.; Müller, Sandra: Strategische Planung für Unternehmensgründer – Anwendung der Szenarioanalyse, in: Corsten, Hans: Dimensionen der Unternehmensgründung. Berlin: Schmidt 2002, S. 71-101.

O'Brien, Frances A.; Meadows, Maureen: Scenario orientation and use to support strategy development, Technological Forecasting & Social Change, 2012, Elsevier GmbH, München

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

Schlake, Oliver: Verfahren zur kooperativen Szenario-Erstellung in Industrieunternehmen, 1. Auflage. Paderborn: HNI-Verlagsschriftenreihe 2000.

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

Seidl, D., &Werle, F.: Strategisches Management und die Offenheit der Zukunft. in V.Tiberius (Hrsg.), Zukunftsorientierung in der Betriebswirtschaftslehre, 2011, Gabler, 287-299, Wiesbaden,

Steinmüller, Karlheinz (Hrsg.): Grundlagen und Methoden der Zukunftsforschung, Werkstatt Bericht 21. Gelsenkirchen: Sekretariat für Zukunftsforschung 1997.

Steinmüller, Karlheinz; Schulz-Montag, Beate: Szenarien – Instrumente für Innovation und Strategiebil-dung. Essen: Z-Punkt GmbH 2003.

van der Heijden, K., 2005. Scenarios: The Art of Strategic Conversation. 2nd. ed. John Wiley & Sons.

von Reibnitz, U., 1988. Scenario Techniques. McGraw-Hill Book Company GmbH

Weimer-Jehle, Wolfgang: Cross-impact balances: A system-theoretical approach to cross-impact analysis, in: Technological Forecasting and Social Change, 2006, Vol. 73, S. 334-361.

Wilkinson, Angela; Kupers, Roland; Mangalagiu, Diana: How plausibility-based scenario practices are grappling with complexity to appreciate and adress 21st century challenges, Technological Forecasting & Social Change, 2012, Elsevier GmbH, München

Wright, George; Ron Bradfield; Cairns, George: Does the intuitive logics method – and its recent enhancements – produce “effective” scenarios, Technological Forecasting & Social Change, 2012, Elsevier GmbH, München

Zinser, Stephan: Eine Vorgehensweise zur szenariobasierten Frühnavigation im strategischen Technolo-giemanagement, 2000, Jost-Jetter Verlag, Heimsheim

Zwicky, F., 1969. Discovery, Invention, Research - Through the Morphological Approach. The Macmillian Company.

10 APPENDIX

ETTIS GLOSSARY VERSION 2

Term	Meaning
Adaptive	A policy solution is adaptive when it is effective in a changing environment by adapting to the new situation
Capability	The ability to address a societal need, consisting of technical artifacts and/or institutional structures which together make up the solution to a societal need
Capability not yet in place	A future capability is an option or the right, but not the obligation, to obtain a capability at a later time, typically with research efforts and cost for this efforts from today..
Challenge scenario	A scenario describing a concrete security challenges. This could be either a threat to security or a source for enhanced security.
Context scenario	Depiction of a future world at an aggregated level, although typically geared to a specific problem area like societal security. It´s an environmental scenario around the specific problem area with strong interactions with it
Delphi method	An anonymous 2-round survey amongst experts to solicit views and build consensus
Disruptive Event	See the definition of “wild card”
Domain	Domain is a specific theme (e.g. cyber security), where threats, needs, capabilities, options and solutions can be identified
Hazard	Results from unintentional acts, like accidents, system failure or natural disaster
Inside-out	Policymakers approach a policy issue a from the inside facing outward
Key factor	Relevant aspects or variables shaping the future of the field that is being analysed (security in generally, domain or focal issue or concrete threat). Key factors are related to scenarios (contextual key factors, threat key factors and challenge key factors). They describe the essential parts of a scenario.
Need	A kind of requirement for response of a specific problem, which occurs if the response is not available A threat scenario interpreted in a given context scenario generates a societal need. It is often mediated through user needs (individual or collective)
Opportunities	An opportunity might either be a favourable or advantageous circumstance, occasion or time, or a chance for progress or advancement. The advantage is usually related to a specific group. Thus this group will consider the favorable event as opportunity.
Options	see the definition of capability not yet in place (the term is abandon as technical term in ETTIS, for simplicity)
Outside-in	Policymakers approach a policy issue from the outside facing inward
Portfolio of capabilities	A group or collection of capabilities
Robust	A policy measure (or capability) is robust if it is effective across different context scenarios
Stakeholders	Both conventional security research end-users and representatives from public and civil society organisations that have some affinity with societal needs
Scenario	
Solution	A solution addresses a (societal) need or (societal) needs
Taxonomy	Arrangement into classifications
Threat	Threats can be a warning that one is going to hurt or punish someone, they can be a sign of something dangerous or unpleasant which may be, or is, about to happen, or they can be a source of danger. In each meaning, the following 3 essential elements are part of a threat: • a harmful event • a cause of this event (either accidently or by intention) • a effect of this event A threat is a subjective interpretation of a specific event. If this event is harmful to a person or a group, this event is considered as a threat from all group members. This opinion is not necessary shared by all other humans. In particular, there might be another group, who take advantage from this event. They usually will not consider this event as a threat. Therefore, threats are always subjective expression of a value.

Threat scenario	Depiction of future developments in a specific field, cyber infrastructure, nuclear and environment. These future developments may also describe aconcrete threat or hazard.
Threat to the EU	A threat results from intentional human activities and is potentially harmful to the security of/in the EU
Time horizon	The length of time between the present and a moment in the future
Trend	A trend in general is a direction, derived from past data. It is usually based on linear pattern, which only work in a specific context. Trends are usually described by time horizon, impact and geographical coverage. Here in this report, a trend is used to make a distinction between trends and wild cards. Trend as a future oriented concept is misleading. It is a well-known fact that it is easy to discover a trend based on historical data on the stock exchange. However it is nearly impossible to learn something about the share price from tomorrow from this.
Topic	Topic is a semantical part of a text. A topic can be a weak signal, a threat, a need, an option, a solution or a capability, besides other semantical functions, usually used in texts.
Weak signals	Weak signals are small and therefore often early signs to events, which point to future threats, opportunities, needs or wild cards. In particular, the weak signals with a potential to be a wild card often points to future strategic discontinuity. Therefore they have a high analytical value for strategic long term planning.
Wild card	Wild Cards are high-impact events that seem too incredible to believe in. Therefore they tend to be overlooked in long term strategic planning. Often it leads even to a decrease in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, "wild cards" refer to low-probability, high-impact events, as introduced by John Petersen author of 'Out of The Blue - How to Anticipate Big Future Surprises'. However more important than probability is, that these topics are not well known and not part of the mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However for strategic long term planning and scenario development they are very important, as they increase the ability in scenario planning, to adapt to surprises arising in turbulent chaotic environments. In trend analysis, they point to trend breaks and tipping points.
Deep uncertainty	Analysts do not know or agree on the appropriate models to describe interactions among system's variables, the probability distributions representing uncertainty and/or to value the desirability of alternative outcomes[10]

[10] Lempert, Popper, and Bankes, *Shaping the Next One Hundred Years : New Methods for Quantitative, Long-term Policy Analysis*.