D.4.1 Threat scenarios

(Results of Interviews and Weak Signal Scanning as well as first results of Focus Group Workshops for the preparation of Threat Scenarios)

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

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

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

Project Acronym	ETTIS
Project full title	European security trends and threats in society
Website	www. ettisproject.eu; www.ettis-project.eu
Grant Agreement #	285593
Funding Scheme	FP7-SEC-2011-1 (Collaborative Project)
Deliverable:	D4.1
Title:	Threat scenarios
Due date:	30 November 2012
Actual submission date:	16 April 2013
Lead contractor for this deliverable:	Fraunhofer INT
Contact:	Sonja Grigoleit Sonja.grigoleit@int.fraunhofer.de
Dissemination Level:	PU

Authors: *Sonja Grigoleit*
Ewa Dönitz
Joachim Klerx
Beatrix Wepner

1 EXECUTIVE SUMMARY 7
2 INTRODUCTION 11
3 INPUT I: INTERVIEWS WITH KEY STAKEHOLDERS 15
3.1 Introduction 15
3.2 Results 18
3.2.1 Nuclear material 19
3.2.2 Cyber infrastructure 25
3.2.3 Environmental issues 31
4 INPUT II: WEAK SIGNAL MINING 40
4.1 Introduction 40
4.1.1 Objectives 40
4.1.2 Approach 40
4.1.3 Search strategy for society threats 42
4.2 Results of scanning for future threats 46
4.2.1 In detail results for the subject "cyber threats" 48
4.2.2 In detail results for the subject "nuclear threats" 52
4.2.3 In detail results for the subject "environmental threats" 57
4.3 Conclusion 60
5 SETTING THE FOCUS WITHIN THE DOMAINS 62
5.1 Nuclear 62
5.2 Cyber infrastructure 63
5.3 Environment 66
6 INPUT III: FOCUS GROUP WORKSHOPS 69
6.1 Stocktaking of the key factors 70
6.1.1 Factors for the Context Scenarios 71
6.1.2 Factors for Cyber Infrastructure 72
6.1.3 Nuclear Waste 73
6.1.4 Environment 74
7 OUTLOOK: APPROACH TO THE DEVELOPMENT OF CONTEXT AND THREAT SCENARIOS 75
8 ANNEX 76
8.1 Interview Guide 76
8.2 Introductory Letter to the Interviewees 84
8.3 Weak Signal scanning 86
8.3.1 Annex 1: Google Trends results for "crisis" 86
8.3.2 Annex 2: Google Trends results for "disaster" 87
8.3.3 Annex 3: Google Trends results for "security" 88
8.3.4 Annex 5: Google Trends results for "nuclear threats" 89
8.3.5 Annex 6: Google Trends results for "environmental threats" 90

List of Figures

Figure 1 - Framework for WP4, with the inputs, minor and major interfaces per task..... 13
Figure 2 - Extract from the ETTIS "Description of Work" (DOW) 14
Figure 3 - Domain and category of the conducted interviews. 16
Figure 4 - Definition of societal need and solution in the ETTIS consortium. 18
Figure 5 - CBRN cycle showing stages, intervention strategies and tools. 25
Figure 6 - System architecture of TIA agent v0.1. 41
Figure 7 - Amount of relative searches for the term "threat" and synonyms. 44
Figure 8 - Quantity of searches, with the term "threat". 45
Figure 9 - Geographic distribution of searches containing the term "threat". 45
Figure 10 - Network structure of the TIA results (symbolic). 47
Figure 11 - Results from topic identification. 48
Figure 12 - Quantity of searches, with the term "cyber threats". 49
Figure 13 - Geographic distribution of searches for "cyber threats". 49
Figure 14 - Quantity of searches, with the term "internet security". 50
Figure 15 - Geographic distribution of searches for "internet security". 50
Figure 16 - Quantity of searches, with the term "black hat" hacker. 51
Figure 17 - Quantity of searches, with the term "nuclear threats". 53
Figure 18 - Geographic distribution of searches for "nuclear threats". 53
Figure 19 - Quantity of searches, with the term "nuclear bomb". 54
Figure 20 - Geographic distribution of searches for "nuclear bomb". 54
Figure 21 - Quantity of searches, with the term "Iran nuclear". 55
Figure 22 - Geographic distribution of searches for "Iran nuclear". 55
Figure 23 - Quantity of searches, with the term "nuclear". 56
Figure 24 - Quantity of searches, with the term "environmental threats". 57
Figure 25 - Geographic distribution of searches for "environmental threats". 58
Figure 26 - Quantity of searches, with the term "extreme weather events". 58
Figure 27 - Geographic distribution of searches for "extreme weather events". 59
Figure 28 - Result of the desk research for exploring the domain cyber infrastructure (related to cyber attack). 65
Figure 29 - Discussing the key factors on context and domain level in focus groups. 69
Figure 30 - 3-step-process for scenario development. 75
Figure 31 - Quantity of searches, with the term "crisis". 86
Figure 32 - Geographic distribution of searches for "crisis". 86
Figure 33 - Rising topics, similar to "crisis". 86
Figure 34 - Quantity of searches, with the term "disaster". 87
Figure 35 - Geographic distribution of searches for "disaster". 87
Figure 36 - Geographic distribution of searches for "security". 88
Figure 37 - Geographic distribution of searches for "social security". 88
Figure 38 - Geographic distribution of searches for "European Security". 88
Figure 39 - Rising topics, similar to "European Security". 89
Figure 40 - Geographic distribution of searches for "nuclear security". 89
Figure 41 - Geographic distribution of searches for "nuclear". 89
Figure 42 - Quantity of searches, with the term "water pollution", from last 9 years 90
Figure 43 - Geographic distribution of searches for "water pollution". 90
Figure 44 - Quantity of searches, with the term "air pollution". 91

Figure 45 - Geographic distribution of searches for “air pollution”. 91
Figure 46 - Quantity of searches, with the term “light pollution”..... 91
Figure 47 - Geographic distribution of searches for “light pollution”. 92
Figure 48 - Quantity of searches, with the term “noise pollution”. 92
Figure 49 - Geographic distribution of searches for “noise pollution”. 92
Figure 50 - Quantity of searches, with the term “genetical engineering”. 93
Figure 51 - Quantity of searches, with the term “food security”. 93
Figure 52 - Geographic distribution of searches for “food security”. 93
Figure 53 - Geographic distribution of searches for “environmental security”. 94
Figure 54 - Quantity of searches, with the term “climate change”. 94
Figure 55 - Geographic distribution of searches for “climate change”. 94
Figure 56 - Quantity of searches, with the term “deforestation”..... 95
Figure 57 - Geographic distribution of searches for “deforestation”. 95
Figure 58 - Rising topics, similar to “deforestation”. 96
Figure 59 - Quantity of searches, with the term “global warming”. 96
Figure 60 - Geographic distribution of searches for “global warming”. 96
Figure 61 - Quantity of searches, with the term “pollution”. 97
Figure 62 - Geographic distribution of searches for “pollution”..... 97
Figure 63 - Quantity of searches, with the term “plastic trash”. 98
Figure 64 - Geographic distribution of searches for “plastic trash”. 98
Figure 65 - Quantity of searches, with the term “Loss of Biodiversity”. 98
Figure 66 - Geographic distribution of searches for “Loss of Biodiversity”. 99
Figure 67 - Quantity of searches, with the term “Rising Sea Levels”. 99
Figure 68 - Geographic distribution of searches for “Rising Sea Levels”. 99
Figure 69 - Quantity of searches, with the term “Population Growth”. 100
Figure 70 - Geographic distribution of searches for “Population Growth”. 100
Figure 71 - Quantity of searches, with the term “invasive species”. 100
Figure 72 - Geographic distribution of searches for “invasive species”. 101

List of Tables

Table 1 - Identifying societal needs across different threat and context scenarios 12
Table 2 - List of the organisations of the interviewees 16
Table 3 - Summary of threats in the area of nuclear material. 22
Table 4 - Capabilities and systemic needs to counter a CBRN attack. 24
Table 5 - High System Level Hazards. Taken from the map of vulnerabilities of the FOCUS project. 32
Table 6 - Natural hazards. Taken from the map of vulnerabilities of the FOCUS project. 33
Table 7 - Important scenarios in the area of environmental threats (from two different interviewees). 36
Table 8 - Statistical review of possible search strategies for “future threats”. 44
Table 9 - Rising topics, similar to “threats”. 46
Table 10 - Overview about topics for potential weak signals in “cyber threats”. 52
Table 11 - Rising topics, similar to “nuclear bomb”. 54
Table 12 - Overview about topics for potential weak signals in “nuclear threats”. 57
Table 13 - Overview about topics for potential weak signals in “environmental threats”. 60
Table 14 - Findings from WP2 related to the domain nuclear. 63
Table 15 - Result of the clustering by key dimensions within cyber security research from WP2 64
Table 16 - Result of the clustering by key dimensions within environmental research from task 2.2 67
Table 17 - Factors for the context 71
Table 18 - Factors for the domain cyber infrastructure 72
Table 19 - Factors for the domain nuclear 73
Table 20 - Factors for the domain nuclear 74
Table 21 - Rising topics, similar to “disaster”. 87
Table 22 - Rising topics, similar to “pollution”. 90
Table 23 - Rising topics, similar to “climate change”. 95
Table 24 - Rising topics, similar to “global warming”. 97

1 EXECUTIVE SUMMARY

The overarching aim of WP4 is the development of **threat scenarios** across different contexts in three domains: cyber infrastructure, nuclear material and environment as a basis for identifying societal needs.

Scenarios provide an in-depth analysis of the key threats; they describe the relevant future developments and events and identify the main actors and their motivations. The developed scenarios help us to identify future possibilities, which are solutions and options related to societal needs.

To pursue this aim we both need context scenarios and threat scenarios: For the identification of the relevant aspects or variables, so called key factors are needed. The **key factors** shape the future of the context (e.g. EU policy, demography, trends & drivers in technology) as well as the concrete threat (e.g. the threat nuclear waste could be described by the factors quantities, infrastructure, global norms and many more).

To derive these key factors the input from 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" will be used:

The **interviews with key stakeholders** (task 4.1) provide us with input regarding current and future threats and societal needs in the three mentioned domains. This insight helps us first to set a thematic focus in each of the three domains and second to derive the key factors for the development of the scenarios.

The interview partners represent conventional security research end-users (police, technical relief teams, ministries of the interior, etc.) as well as public and civil society organizations engaged in societal needs on a general level (religious communities, NGOs, etc.).

Apart from the interviews we analysed reports and deliverables of recently completed projects (e.g. ESRIF; FOCUS, FESTOS, FORESEC, ENISA – Threat Landscape) which have a similar focus as ETTIS. Thereby we want to make sure that we are not duplicating or even reemphasizing their results.

It was observed that the statements of the interviewees gave new insight and new points of view to the systematics of threats described in previous reports. The interviewees added urgency to the mentioned threats, breathed life into them and gave easy-to-understand examples.

In the domain of **nuclear material** the interviewees mentioned state actors (e.g. threat of nuclear weapons) as well as non-state actors (e.g. theft of nuclear material during transport, civil radioactive sources).

In the domain of **cyber infrastructure** a broad range of threats were mentioned. In general it was stated that due to the dramatic changes and growing complexity in ICT technology the gap between developing risks and preventive and protective capabilities seem to become bigger each day. It was also said that the type of actor is changing and moving into the direction of big criminal organizations or even state-enabled unities.

Environment is also a very complex domain. The interviewees mentioned a lot of high system level hazards like climate change, loss of biodiversity, change in land use and inefficient use of natural resources. On a more differentiated level the interview partners especially mentioned climatic events (like heat waves, flooding and storms), tectonic events (like earthquakes) and environmental pollution (e.g. chemical accidents, excess use of nitrogen compounds in agriculture, depletion of fish stock).

In general the interviewees stated in all three domains that the awareness and the education of the society is a key **need** and most important for the resilience of the society. They also mentioned a broad range of **solutions** which were partly of technological nature (e.g. warning systems, build-in IT security, proper system of dismantling and disposal of nuclear weapons), but in many cases of a more general nature (e.g. promotion of interdisciplinary communication and networking, cooperation even outside the "comfort zone" of likeminded states, international rules and standards).

In the course of preparing the **focus group workshops** setting the focus within the domains cyber infrastructure, nuclear and environment was an important step (see chapter 5). In particular the domains nuclear and environment are very broad and include a wide range of different issues. Based on the findings of the desk research analysis of the relevant future studies, the findings of the WP2 (D.2.2) as well as first results of the interviews with key stakeholders and the weak signal mining the focus was set as follows:

- Domain nuclear: i.a. nuclear power plants, use of nuclear material, nuclear accidents, waste management risks and dumping of hazardous waste.
- Domain cyber infrastructure: i.a. cyber attacks and cyber crime, social network and privacy, information risks, data storage, vulnerability of existing and new information technologies (e.g. mobile phones).
- Domain environment: i.a. loss of biodiversity, invasive alien species, water pollution, land use and pollution, deforestation and soil erosion, population growth as well as potential conflicts related to the resource scarcity and resource distribution.

The next step for the preparation of the focus group workshops was the stocktaking of the key factors, which are relevant for the context as well as for each domain and which should be described in scenarios (see chapter 7). Regardless of the domain a broad range of different aspects from the following fields are frequently named: EU policy, EU development, socio-cultural developments, trends and drivers in technology, research landscape, ecology and sustainability or economy. However there are also specific research fields for each domain, like sources and types of attacks or attack targets and vulnerability (cyber infrastructure), handling of disposal and transport or material control and accounting procedure (nuclear) and agriculture or forestry (environment).

The main goal of the text mining in WP4.2 was to identify possible future threats on the internet. As "future threats" are a very abstract concept it is not possible to search these threats with a simple semantic search strategy. Therefore, a two-step search strategy was developed. In a first step a community was identified; in which members of the community publish content about future threats on the internet. In a second step the content was clustered to find out about the main topics of possible future threats and an in depth analysis of these topics was conducted to get hints about possible weak signals for future threats.

The threat identification agent (TIA) identified about 80,000 links in sites containing the phrase „future threats". From these links all were compared to the search strategy of TIA by downloading the sites, parsing the html and tested whether the term "future threats" was in this text. About 6,000 sites were identified, that complied these criteria. TIA discovered that the "future threats" network is not really interconnected and has an unknown number of subnets. Threat discussions on the internet seem to be context dependent. The number of discussions increases around a threat event (such as Fukushima nuclear disaster) and decreases after the event.

The in depth analysis of WP 4.2 brought up the following possible terms for indicating weak signals:

- *cyber threats:* "botnet", "trojan horse", "stuxnet", "zero days" exploit, "smurf attack" "black hat" hacker, "cyber warfare", "sykipot", "elderwood platform", "cyber espionage", "aurora trojan"
- *nuclear threats:* cyber threats of nuclear power plants, "nuclear plant" hacked, "nuclear terror", "nuclear waste"
- *and environmental threats:* "extreme weather events", "water pollution", "air pollution", "light pollution", "noise pollution", "deforestation", "plastic trash", "oceanic dead zones", "explosive population growth", "invasive species", "genetical engineering", "man made viruses", "biomimetic robots", "genetic engineering" threat, "genetic engineering" food, "threats to food security"

Derived from the experience from the first web crawling, two improvements are foreseen for the second web crawling. First, as the heterogeneous network structure caused, that the list of potential weak signals for future threats is not extensive, the second web crawling will run with an adapted crawling strategy to improve the network structure.

Second and finally, for some topics the internet can be a better source for content than for other topics. For cyber security for example a lot of very detailed threat information can be found. For nuclear threats it seems that some important information is missing or only available in expert libraries. For environmental threats there is a huge amount of information about threats on the internet, but this information is in different subnets. The search strategy of our agent needs to be adapted to deal with this.

2 INTRODUCTION

The overarching aim of WP4 is the development of threat scenarios across different contexts in three domains: cyber infrastructure, nuclear material and environment as a basis for identifying societal needs. For this purpose the following objectives will be pursued:

- identifying key threats/hazards to society for further analysis,
- developing context scenarios as the general framework conditions for these threat scenarios,
- developing threat scenarios, among which at least three scenarios around the domains nuclear, cyber infrastructure and environment and
- identifying and anticipate future user needs and societal needs with the key uncertainties

Scenarios provide an in-depth analysis of the key threats for the proposed domains cyber infrastructure, nuclear and environment. They describe the relevant future developments and events and identify the main actors and their motivations. Scenarios examine critical security related developments and uncertainties in two ways: higher-level (context scenarios) and domain-specific (threat scenarios). Particularly the societal, political and economic environment, covered mostly by the context scenarios, is largely unpredictable. Scenarios offer a help to deal with this uncertainty. Depending on the different context the substance of the threats will be examined.

We will consider threat scenarios across different context scenarios for three main reasons: First, threat scenarios may address different societal needs in different context scenarios. Second, the effectiveness of solutions may also differ widely across different contexts. Third, solutions should be robust and adaptive in order to address a wide range of societal needs. Scenarios offer different future perspectives, help us to identify future option spaces and thereby enable testing the robustness of the solutions and options. For testing the robustness it is recommended to create at least 3-4 context scenarios and at least 3-4 threat scenarios for each domain. The same context scenarios will be used for all domains.

The future exploration using scenarios supports the identification of future possibilities, which means solutions and options related to societal needs. The relationship between societal needs, threat and context scenarios is illustrated in Table 1 below. Note that the matrix includes a column for interpreting each threat scenario in relation to today's context, i.e. today's society.

	context today	context scenario A	context scenario B	context scenario C	...
Threat scenario 1 set of future projections of the key factors (specific to the threat)	present situation	context based threat scenario 1A	context based threat scenario 1B	context based threat scenario 1C	...
	societal needs	societal needs	societal needs	societal needs	...
Threat scenario 2 set of future projections of the key factors (specific to the threat)	present situation	context based threat scenario 2A	context based threat scenario 2B	context based threat scenario 2C	...
	societal needs	societal needs	societal needs	societal needs	...
Threat scenario n	societal needs	societal needs	societal needs	societal needs	

Table 1 - Identifying societal needs across different threat and context scenarios

Basically scenario development proceeds via two steps: In the first step, context scenarios will be created followed by the second step - the creation of threat scenarios. For the identification of the relevant aspects or variables, so called key factors are needed. The **key factors** shape the future of the context (like security in general) as well as the concrete threat. The key factor in the context scenarios have overarching relevance for the field of security and are equally important for the domains cyber infrastructure, nuclear and environment. The context analysis may include the identification of emerging trends and global developments. The key factors for the threat scenarios describe the specific object of analysis and shall apply only to one of the domains.

To derive these key factors the input from 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” will be used:

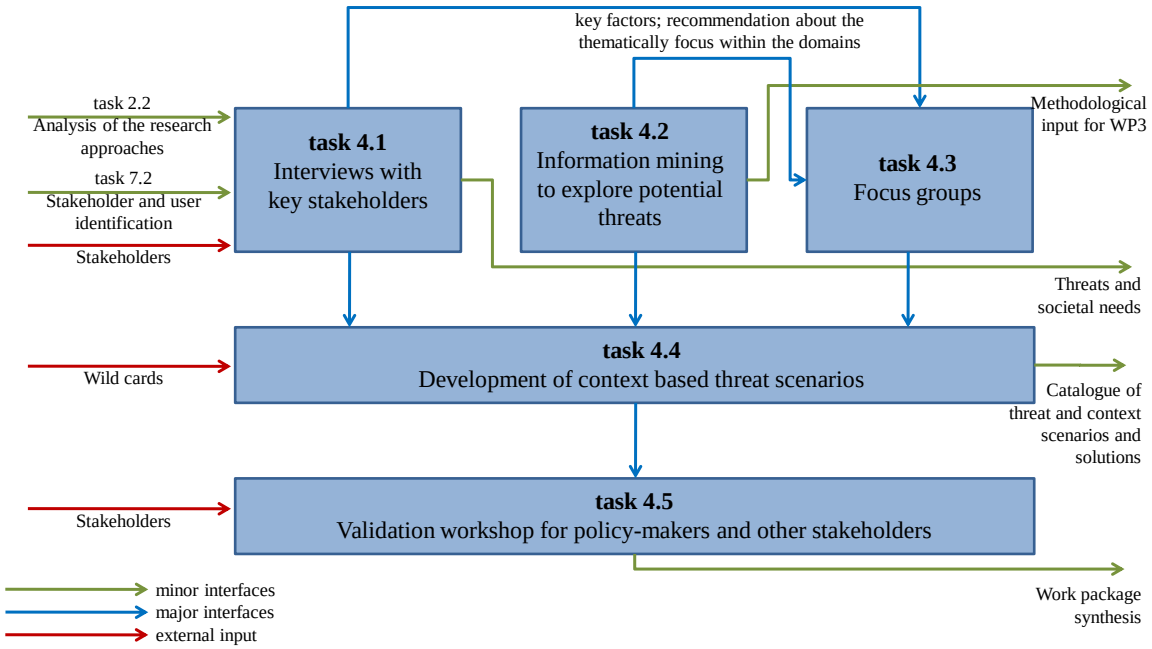


Figure 1 - Framework for WP4, with the inputs, minor and major interfaces per task

The **interviews with key stakeholders** (task 4.1) provide 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.).

We are conducting the interviews in two phases. In phase 1 we set the focus on the identification of threats and needs and mainly conducted interviews with conventional security research end-user. The aim of the first phase of interviews is to provide the focus group workshops with input 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 will take place after the focus group workshops when the first scenario drafts are ready. In the second phase we will discuss the needs and security solutions with stakeholders. For the second phase we will mainly interview representatives from public and civil society organisations engaged in societal needs.

IT-based weak signal scanning (task 4.2) will be used to explore emerging threats and societal needs based on sources from internet. The weak signal scanning can deliver important information about the emerging aspects within the domains and in that way help by specifying the thematic focus within the domains.

The **focus groups** (task 4.3) will deliver input to the identification of threats, trends and needs and to the development of scenarios as well as to a deeper understanding of the contexts of the scenarios. The focus groups will contribute to an analysis to identify and structure all factors influencing the development in present and future time.

Task 4.1: *Interviews with key stakeholders (M7-M11)*
Task 4.2*: Information mining using advanced IT tools to explore potential threats (M7-M20)*
Task 4.3: *Focus groups (M10-M14)*
Task 4.4: *Development of context based threat scenarios (M13-M19)*
Task 4.5: *Validation workshop for policy-makers and other stakeholders (M17-M19)*

D4.1) *Threat scenarios: A report which includes a set of threat scenarios at two levels: context and situational, as well as an analysis of key threats and associated needs (societal and user) which emerge from the scenarios. The report will contain annexes on the results of interviews, focus groups and weak signal mining. [month 11]*
D4.2) *Methodology Note: The internal deliverable will feed back experiences from WP 4 to WP 3, for refining the methodology developed. [month 20]*
D4.3) *Focus group report: A summary report on the findings made through the focus group, including indication of consequences for the further development of the research. [month 14]*
D4.4) *Catalogue of threat scenarios: Complete narrative threat scenarios produced through the scenario development of Task 4.4. [month 19]*
D4.5) *Validation report: Report from the validation workshop, including commentary and reassessment of the narrative threat scenarios. [month 19]*

Figure 2 - Extract from the ETTIS "Description of Work" (DOW)

The ETTIS DOW describes D 4.1 (due in M11) to be a report about threat scenarios.
However, the development of the threat scenarios is to be carried out in Task 4.4 (M13-M19). Therefore we decided that D4.1 should contain mainly the results of Task 4.1 and additionally the first results of Task 4.2 and Task 4.3.

The threat scenarios will be developed in Task 4.4. The results of that task will be published in D4.4.

3 INPUT I: INTERVIEWS WITH KEY STAKEHOLDERS

3.1 INTRODUCTION

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

This deliverable D 4.1 describes the approach and the result of the first phase of the interviews. The second phase of the interviews will be done on the basis of the first scenario drafts and will be reported in deliverable D 4.5. Due to time constraints and the need to deliver first results of the interviews to the already started task dealing with the focus group workshops, this first phase only includes 18 interviews. The second phase will contain more interviews to refine the final picture.

As described in the DOW we also planned to conduct interviews with coordinators of previous projects engaged in current and future threats and societal needs in order to not duplicate ore even reemphasise their results. Instead of conducting interviews we decided to analyse the deliverables and final reports of the relevant projects. The following projects and forums were found relevant for our research (i.e. they have a similar focus as ETTIS and the projects were not completed long ago):

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

In phase 1 we set the focus on the identification of threats and needs and mainly conducted interviews with conventional security research end-user (see Table 2).

We aimed at reaching a balanced mixture both of the categories of organisations (governmental and civil society organisations) as well as of the thematic domain (cyber infrastructure, nuclear material and environment). As the domain "environment" is a quite broad collective term (e.g. including threats ranging from natural and man-made disasters over pandemics and resource scarcity to climate change), we conducted most of the interviews in this domain (see Figure 3).

Organisation	Country	Domain	Category
Oxfam	*Germany*	*environment*	*CSO*
Federal Agency for Technical Relief	*Germany*	*environment*	*Government*
Red Cross	*Germany*	*environment*	*CSO*
Federal Office for Civil Protection	*Switzerland*	*environment*	*Government*
Catholic Church	Germany	environment	CSO
Environmental defense fund	USA	environment	CSO
Dutch Ministry of Infrastructure and the Environment	*Netherlands*	*environment*	*Government*
International Red Cross	*Sweden*	*environment*	*CSO*
International Physicians for the Prevention of Nuclear War	USA	nuclear	CSO
Federal Environment Ministry	*Germany*	*nuclear*	*Government*
United Nations Institute for Disarmament Research	Switzerland	nuclear	Government
Information Security Association	*Italy*	*cyber*	*CSO*
Dutch Ministry of Economic Affairs	*Netherlands*	*cyber*	*Government*
Privacy International	UK	cyber	CSO
International Alert	UK	general	CSO
Scandinavian Islamic Organisation	Sweden	general	CSO
Swedish Civil Contingency Agency	*Sweden*	*general*	*CSO*
Swedish Armed Forces	*Sweden*	*general (+cyber)*	*Government*

Table 2 - List of the organisations of the interviewees (Organisations printed in italics are mainly seen as end-user).

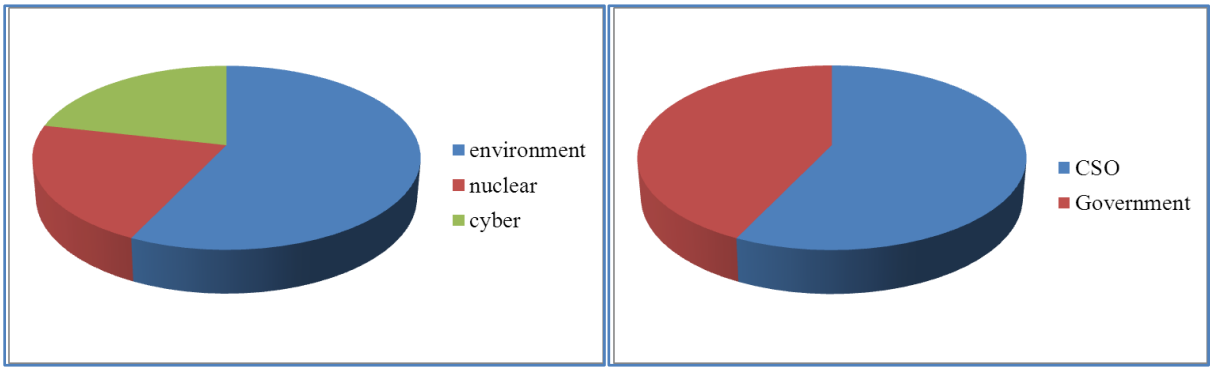


Figure 3 - Domain and category of the conducted interviews.

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

We also took into account the different backgrounds of the interviewees and prepared an introductory letter containing explanations of the aim of the interviews and the used terms, like threat, need and security solution (see chapter 8.2).

The following list contains the questions for experts in the area of nuclear material. The questions for the other two domains are rather similar – the only difference is the time horizon in question 2. We used a time frame of 5 years for cyber infrastructure and 15 to 20 years for nuclear material and environment:

Threats & Hazards:

1. Which threats & hazards do you see in the area of nuclear material?
   Choice of further questions:
   a. We want to get a clear and complete picture of the threats and hazards in the area of nuclear material. What do we need to take into account?
   b. Is it possible to define organisations/groups who are responsible? – Which aims do they pursue?
   c. How vulnerable is our society regarding these threats & hazards and what areas/sectors are most vulnerable to these threats?

2. We are also interested in the development of the threats and hazards in the next 15 or 20 years. How do you think will the threats and hazards you have mentioned develop in this timespan?
   Choice of further questions:
   a. Will there be new threats & hazards?
   b. Will the vulnerability of the society change and why?

Needs:

3. What do you see as the societal needs to result out of the before mentioned threats & hazards?

Security Solutions:

4. Which capabilities do we need to address these societal needs?
   Choice of further questions:
   a. Which technical systems do you suggest?
   b. Which institutional structures are needed?

5. What capabilities do you think we should aim at in the future?
   Choice of further questions:

a. In which research areas would you suggest to invest today?

6. If we combine all these capabilities you mentioned to a security solution - do you see secondary effects of this security solution on the society?
   Choice of further directions:
   a. Financial limits
   b. Ethical & privacy issues
   c. Other risks

3.2 RESULTS

A general result of the interview has been that the interview partners didn't see the necessity to distinguish between "needs" and "solutions", although the members of the ETTIS consortium (interviewer) explained the difference.

- ***Societal need****: A threat scenario interpreted in a given context scenario generates a societal need. It is often mediated through user/ stakeholders needs (individual or collective). A need is some kind of requirement for response to a specific problem.*
- ***Solution****: A solution addresses a societal need or societal needs and is composed of capabilities.*
- ***Capability****: Capability refers to the ability to address a societal need and consists of technical artifacts and/or institutional structures*

Figure 4 - Definition of societal need and solution in the ETTIS consortium.
Source: ETTIS, A Preliminary Methodological Framework, Deliverable WP3.1, 2012.

We observed that the boundaries between "needs" and "solutions" were blurred. In most cases when asked for the societal needs the interviewees 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. Thus the ETTIS team shall work in the upcoming tasks on the two terms and make sure that we are able to communicate successfully with all stakeholders.

As the number of interviews (18) in the first phase of interviews is not large enough to make statements about the relative significance or frequency of the single threats, we decided to structure the results of the interviews in the following way:

We analysed the reports and deliverables of the relevant projects (e.g. ESRIF; FOCUS, FESTOS, FORESEC, ENISA – Threat Landscape) and decided upon a reasonable structure for each particular domain (nuclear material, cyber infrastructure and environmental issues). Along this structure we included all the statements of the interviewees. It was observed that the statements gave new insight and new points of view to the systematics of threats described

in previous reports. The interviewees added urgency to the mentioned threats, breathed life into them and gave easy-to-understand examples.

The following chapters contain the results for each domain.

3.2.1 Nuclear material

In this chapter reports from completed EU projects with the focus on threats, needs and/or security solutions were exploited (European Security Research & Innovation Forum –ESRIF; European Security in Light of Evolving Trends, Drives and Threats – FORESEC; Foresight of Evolving Security Threats Posed by Emerging Technologies – FESTOS). The results were combined with three interviews already completed in the area of nuclear material.

3.2.1.1 Threats

Nuclear threats were discussed in detail within the working group 6 (CBRN) of the European Security Research & Innovation Forum (ESRIF).[1] In general CBRN threats and challenges were divided into two categories – state actors and non-state actors.

States were said to be the actors with the best capabilities to maintain sophisticated weapon programs.[1] On the other hand states are probably the least likely actors to actually use CBRN weapons towards EU territory, taking into account that states are generally rational actors that will have several constraints against the actual use of CBRN weapons.[1] But it should be recognized that the control over CBRN weapons in certain states could change quickly because of political unrest, sabotage or natural disasters.[1]

The researchers of the FORESEC project were very concerned that **Iran** will develop a nuclear bomb.[2] If Iran does develop nuclear weapons, the probability that it will intentionally use them or transfer them to terrorist proxies is small.[3] However, the Iranian nuclear programme has the potential to trigger a regional proliferation cascade in the Gulf and the wider Middle East.[3]

One interviewee is particularly concerned with **nuclear weapon arsenals**. Currently there are nine nuclear weapon states – the largest still the US and Russia. Israel has an undeclared nuclear arsenal and is therefore at the heart of the problem in Middle East. India and Pakistan are new nuclear weapon states and the DPRK has a small arsenal but its withdrawal from non-proliferation has raised concerns.

[1] ESRIF, Final Report, Dec. 2009.
[2] FORESEC – Cooperation in the Context of Complexity: European Security in Light of Evolving Trends, Drivers and Threats, Final report, 2009.
[3] FORESEC Deliverable D 4.5 – Report on European Security: Trends, Drivers, Threats, 21. Aug. 2009.

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

One interviewee sees a continuum of ways in which nuclear weapons pose a problem. The most extreme end is a **nuclear war** due to accident, miscalculation, an error prone command and control, "broken arrow", etc. Nobody expects that to happen, but the arsenals are maintained at those levels.

A single use against a city is regarded to be more plausible. It could be a decision out of desperation in critical regions.

Non-state actors are typically terrorist organizations.[4] In relation to non-state actors there is a relatively high probability that a terrorist attack involving C, B or R-weapons will take place in Europe over the course of the next 10-20 years.[4] The use of N-weapons is less likely.[4] The use of CBRN agents has a major psychological dimension. In some cases, the objective of a non-state actor could be to simply cause panic and fear.[4]

One of the interviewees sees a potential threat in a **terrorist attack on a nuclear site**. At the moment they are no specific indications of an imminent attack. But it is assumed that we have to be generally prepared against an attack driven by cultural or religious backgrounds. The threat due to right-wing or left-wing extremist groups does not play a major role.

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

Another issue is the security of **existing material**, that would include weapons as well as civilian material (e.g. radioactive waste of nuclear power plants, radioactive sources from hospitals or material inspectors). In the military domain (without counting nuclear power) there are globally transfers of tens of tonnes of material. The sheer number creates the possibility of some material being misplaced, lost or stolen.

One interviewee said that specifically in the non-civilian domain there is very little that could provide the security standard. Each country does it best to protect its material, but there is no clear picture of how good these efforts are.

There are international agreements that set out some responsibility; e.g. there are conventions for physical protection and a convention against terrorism etc. The basic problem is that these

[4] ESRIF, Final Report, Dec. 2009.

impose very few specific obligations on physical protection. The only legally binding obligation is to protect civil material in international transports. Everything else is up to the individual countries.

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

Technological progress in the radiological/nuclear field takes place at a very rapid pace.[5] A downside to these technological developments is that they make it easier to develop, acquire and deliver RN weapons.[5] In the area of radiological and nuclear dual-use technology the following developments should be mentioned:[5]

- Already existing installations (research reactors) could be used for clandestine irradiation of raw material
- Neutron generators are getting smaller and cheaper and may be used in parallel to their actual purpose
- Accelerators (particularly compact cyclotrons) will get smaller, easier to operate and cheaper
- Atomic Laser Isotope separation: the technique should be monitored; it will be possible to achieve high enrichment with just a few steps
- Use of Nanosieves: an aspiring technique which may be used for enrichment
- Modern separation systems with remotely controlled machines and appropriate hot cells will be available worldwide for processing burned (used) fuel rods
- New techniques for aerosol technology may be used for dispersion of radioactive or nuclear material

In the opinion of experts of the FESTOS project new nuclear technology materials[6] can be abused and bring new threats because of potential utilisation for making nuclear (both fissile and dirty) bombs by terrorist groups.[7]

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

One interviewee said that there are different directions. On the one hand the nuclear weapons states have modernization plans. Although the **US and Russia** are reducing the numbers of nuclear weapons, they are only getting rid of the old ones and are investing in new generation

[5] ESRIF, Final Report, Dec. 2009.

[6] The following new materials and processes were discussed during the FESTOS project: organic superconductors, materials with special magnetoresistive effects, radiation-induced segregation, Uranium silicide fuels which require only low-enrichment, new solid lubricants, nanocrystalline diamond films.

[7] FESTOS – WP2: Horizon scanning – Deliverable D2.3: Final report on potentially threatening technologies, March 2009.

designs and missions. If this continues it will be very difficult to stop other countries from starting their own nuclear weapons programme.

On the other hand there are growing groups of non-nuclear states in and outside the Nuclear Proliferation Treaty (NPT), who have a new interest in the humanitarian consequences of nuclear weapons. In March there will be a conference in Oslo about the **humanitarian consequences of nuclear weapons**. The aim has to be to ban and eliminate nuclear weapons.

Another expert also didn't expect any radical changes and thinks it will be a slow progress. The interviewee hopes that there will be a progress in the development of institutional arrangements for disarmament that could help reduce the distrust in the system. That in turn would help build better relationships, especially in Europe, and that would have a positive effect on **nuclear disarmament**.

States (nuclear weapons)	
	Usage of nuclear weapons (act of desperation, loss of control, accidents)
	(Possible) new nuclear states (DPRK, Iran)
	Slow disarmament in nuclear states arouses desire in other states to get nuclear weapons
Non-state actors	
	Terrorist attack on a nuclear sites
	Theft during transport of nuclear weapon materials
	Theft during transport of civil nuclear material
	Civil radioactive sources (hospitals, research reactors, materials inspectors..)
Technological developments	
	Devices (neutron generators, accelerators) get smaller and cheaper
	New technologies of enrichment
	New techniques of dispersion of radioactive or nuclear material

Table 3 - Summary of threats in the area of nuclear material.

3.2.1.2 Societal Needs

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

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

The events (e.g. accidents, terroristic activities, nuclear war) all have a low probability but a high consequence. Therefore we need a **good crisis management** to be prepared for the case of a release of radioactivity.

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

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

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

3.2.1.3 Solutions

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

One interviewee said that on a technical level a proper system for the **dismantling and disposal of nuclear weapon** materials is needed. They have to be secured and kept in an environmentally responsible way. It was also suggested to spend additional research funds in the area of "safe disarmament" and into the handling and storage of nuclear weapons materials.

Another interviewee believes that there is no technical solution for the problem of the misuse of nuclear material. All the technical attempts (like alternate fuels for nuclear power plants or surveillance systems) only give a false sense of security. To make progress in the area of nuclear disarmament and the security of nuclear material the only way is seen in **cooperation** – in working institutional structures, exchange of information and inspection of sites.

In the area of **terrorist CBRN attacks** the working group 6 (CBRN) of the European Security Research & Innovation Forum (ESRIF) spent a lot of efforts in identifying capability gaps as well as research and innovation priorities. For an easier classification ESRIF used a CBRN cycle covering the stages assessment, prevention, preparedness, response, mitigation and recovery (see Figure 5).

Stage of CBRN cycle	**Capabilities**
Threat assessment	
	CBRN integral threat assessment (actor analysis, information management,..)
Prevention	
	Counter proliferation and counter terrorism (global treaties, awareness of dual-use potential, border-security)
Preparedness	
	Monitor the illegal attempt to use CBRN material for terrorism purposes (detection technologies, international standardization, training)
Response	
	Crisis management (situational awareness, integrated communication systems)
	Detection and identification of CBRN agents (including forensic aspects)
	First Responders (Training, Personal Protective Equipment)
	Contamination containment
Mitigation	
	Medical treatment (generic and specific)
Recovery	
	Decontamination and remediation of the impacted areas
	Psychological and social resilience (effective risk communication, emergency psychological support)

Table 4 - Capabilities and systemic needs to counter a CBRN attack.
Source: ESRIF, Final Report, Dec. 2009.

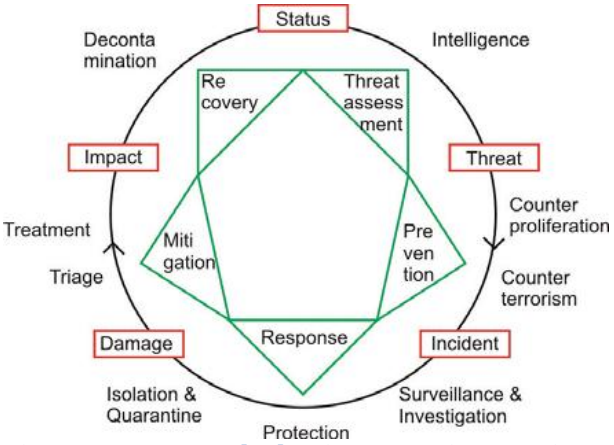


Figure 5 - CBRN cycle showing stages, intervention strategies and tools. Source: ESRIF, Final Report, Dec. 2009.

3.2.1.4 Secondary effects of security solutions

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

Another interviewee mentioned that for example in nuclear sites a lot of security measures were implemented which all have **data protection & privacy** aspects. People have to hand over their identity cards as well as mobile phones. They were searched and everywhere inside the building there are video cameras. But nobody complains about the measurements. The interviewee thinks that it is crucial that the stakeholders were well informed about why and how the security measurements were implemented.

3.2.2 Cyber infrastructure

In this chapter reports from completed EU projects and forums with the focus on threats, needs and/or security solutions were exploited (European Security Research & Innovation Forum –ESRIF; Foresight Security Scenarios – FOCUS; European Network and Information Security Agency (ENISA) Threat Landscape). The results were combined with three interviews already completed in the area of cyber infrastructure.

3.2.2.1 Threats

EU's cyber security agency ENISA[8] has published a comprehensive cyber threat landscape analysis in 2012, summarising over 120 threat reports.[9] In the report the current top cyber threats have been identified.[10] Current threat trends have been derived from the comparison of current threat information with the situation in the last years.[10] Also a number of threat trends for emerging areas of information technology have been formulated.[10] The areas considered are mobile computing, social media/technology, critical infrastructure, trust infrastructure, cloud and big data.10 In each of this area it was indicated, if the specific threats (see list below) are declining, stable or increasing.[11]

The identified current top ten threats are:[9]

1. Drive-by exploits (malicious code injects to exploit web browser vulnerabilities)
2. Worms/trojans
3. Code injection attacks
4. Exploit kits (ready to use software package to automate cybercrime)
5. Botnets (hijacked computers that are remotely controlled)
6. (Distributed) Denial of Service attacks (DDoS/DoS)
7. Phishing (fraud mails and websites)
8. Compromising confidential information (data breaches)
9. Rogueware/scareware
10. Spam

Cyber risks were also studied by working groups with a more holistic view on security research (e.g. ESRIF, FOCUS, FESTOS).

They concluded that with the **dramatic changes in ICT technology** the gap between developing risks and preventive and protective capabilities seems to become bigger and bigger.[12] All notable national and international organizations have taken notice of the risks and have formulated resolutions and strategies, but concrete and adequate protection, defence and counter measures are still missing.[12]

One interviewee stated that the **complexity of systems** is increasing and with it the potential to misuse the system. The IT market is constantly changing with many new systems on the market. ENISA also stated that all trends in threats and vulnerabilities show an exponential increase over time.[12]

[8] European Network and Information Security Agency
[9] ENISA, New report on top trends in the first cyber threat landscape by EU's cyber agency ENISA, press release, 8. Jan. 2013.
[10] ENISA, ENISA Threat Landscape, Responding to the Evolving Threat Environment, 2012-09-28.
[11] ENISA, ENISA Threat Landscape, Responding to the Evolving Threat Environment, 2012-09-28; see table on page 8.
[12] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

Nowadays, cyber-criminals seem to be more motivated by a desire to gain financially than to cause electronic vandalism. They design malicious codes to use infected machines to accomplish objects, such as stealing credit cards numbers, sending spam or providing an "unguarded" entry into the organisation's network.[13] The threat of **cyber criminality comprise a broad range**: from direct threats to individuals (e.g. online child sexual abuse) to threats to the national security of entire countries (large scale attacks on information systems) and occasionally a global impact cannot be excluded.[13] Threat trends clearly move into the direction of **state or state-enabled actors** and serious international crime.[14]

One interviewee said that in the area of cyber threats there are several players. There are still single hackers. But at the moment there is a huge shift in this area. Today behind these hackers are **big organizations** with a lot of money. For example there are organisations in South America, who formerly have been active in the area of human trafficking or drug dealing, are now working in cybercrime, which is quite lucrative.

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

Apart from the cyber threats mentioned in the ENISA list above ESRIF especially mentioned **identity theft**, which is increasing spectacularly.[13] This is also the primary threat to e-ID schemes.[13] Thus the EU is facing several challenges related to e-ID (for e-Services and for e-Travel documents), where identification, authentication and signature are mandatory.[13]

It is also seen as a problem by one of the interviewees that the providers often make use of so-called **2nd or 3rd line contracts**. It is not always clear whether these systems contain bugs or "backdoors" (see the Huawei case for an example[15]).

Another issue is that software is often purchased "off the shelf", only to be customized afterwards. Often systems are put on the market as soon as they are "acceptably solid". Their vulnerability however at this stage is often high.

A further vulnerability is the increased usage of **mobile devices** and systems. Everything "smart" can be connected to the internet and thus potentially be misused by third parties, if adequate safety features are absent or turned-off.

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

[13] ESRIF, Final report, Dec. 2009.
[14] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.
[15] William Wan and Craig Timberg, China slams congressional charges against its telecom firms Huawei and ZTE, Washington Post, 9. Oct. 2012.

Another interviewee sees the main threat in the usage of **SCADA** (supervisory control and data acquisition) as an industrial control system. The problem is that the life cycle of these machines are very long (around 20 years), so the computers who are working with these machines renew very slowly. But the main problem is the lack of awareness. The people working with these machines do not realize that they have a security problem; therefore the security in these machines often lags 10 years behind the state-of-the art. The companies want to get remote access to their automation processes and are using "toys" like tablet PCs. The tablets are not designed to control industrial processes or even nuclear plants.

One interviewee sees the challenge that the **trust put in consumer devices**/services will be hampered, if these devices are misused (e.g. security breach at DigiNotar, a Dutch certificate authority[16]).

There is also seen an increasing potential for "movements" (good but also bad ones) in societies, which are strongly supported by **social media**.[17] It is hard or even impossible to identify causes, origins, leaders, organizations of "movements" of people and thus negotiations are denied.[17]

The interviewees were also asked on their views on how the threats and risks will develop in the next 5 years. One interviewee stated that they are observing that the amount of crime rises every 6 month by 300%. Both the gravity of the threats as well as the costs of the incidents is growing fast. They think that within 3 years we will reach a **global peak in IT-usages**. They assume that from then on the disadvantage of the internet will be bigger than the advantage and the users will start to withdraw themselves from the internet. It was said that at the moment the internet is not capable of adapting - for example the prosecution of cyber criminals is not working well.

In general the interviewees found this question rather hard to answer. It is not easy to see if the current dynamic will change and will lead to increased awareness and more secure platforms. In this optimistic scenario the industry will be held accountable and the policy makers will become wiser. But it could also happen that people reject technology or that they say "so be it" and continue to use the fragile technology, which could lead to a terrible outcome.

3.2.2.2 Societal Needs

The interviewees said that we basically need 3 things.

1. We need **education and awareness**. The people should be educated in internet security from play school onwards.

[16] Wikipedia, DigiNotar, http://en.wikipedia.org/wiki/DigiNotar, seen at 23. Jan. 2013.
[17] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

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

3.2.2.3 Solutions

The security of the information and communication technology (ICT) was also an important part of the work of the ESRIF. The forum came to the conclusion that ICT networks need research to increase systemic resilience, e.g. via intrusion detection, "self-healing" networks or semi-intelligent data filtering.[18] ESRIF also mentioned the following required capabilities:[18]

- Network capability to trace illegal activities in cyberspace back to its origin
- Detection and blocking of websites potentially harming citizens and issues of common interest (note of the author: *this might also have secondary effects*)
- Parameterisation methodologies for detection of suspicious cyberspace behaviour (note of the author: *this might also have secondary effects*)
- Development of international applicable unique interfaces, protocols, connectors, etc. for trusted exchange of sensitive information
- Influencing the behaviour of cyberspace users to reduce their vulnerability against actions with hostile intent (new anti-virus programmes with online investigation modules for the identification of senders of messages, methods for alerting the users to the potential risks of their ICT behaviour)
- A legal basis to control the misuse of the internet system and to protect privacy

[18] ESRIF, Final report, Dec. 2009.

- Increased robustness of electronic identities and more stringent authentication processes
- Methods for increasing user awareness on the potential risks of ICT behaviour

The FOCUS project also identified several consequences out of their described threat landscape.[19] The researchers stated that cyber risks require a **dynamic strategy** which is able to react in time.[19] They said that cyber risk countermeasures require solutions which work fast and **across disciplines**, commercial sectors and government administrations.[19] Cyber threat counter programmes will increasingly require **governmental and EU legislation** and regulation; to wait for voluntary action will not suffice.[19]

One of the interviewees said that it is of key importance to form institutional structures at the international level. It is important to create a **level playing field of institutions**, so that people/organizations can exchange information at the same level and with similar mandates. The Computer Emergency Response (CER) teams or national cyber security centres in each country have a different structure and mandate. If you want to make sure that vulnerabilities are better addressed, particularly cross-border, this will have to be harmonized.

The FOCUS team also concluded that a **strategy of de-netting of societies**, administrations and critical infrastructures, of building redundancies and fall-back positions (even manual ones) will become mandatory.[19] One interviewee also sees the particular need for a European infrastructural network with a high level of redundancy (excess capacity, the ability to fall back on additional capacity when a disruption occurs).

One interviewee stated that it is important that we have to follow **international standards** and that we use hardware with **build-in security**. Another interviewee sees rigorous testing of technologies as important. Randomised controlled trials might be helpful, but systems tend to get properly attacked when they are out in the wild being fully in use.

A main problem is also seen in **user authentication**. This is important so that you can prove that someone is innocent or was doing cybercrime. The interviewee claimed that today with a good lawyer you can always say that the log-files were forged.

Another interviewee said that we need harder ways of going after the **technology producers** and holding them accountable. We need to be able to ask Google or Microsoft what they are doing to make their devices secure.

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

[19] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

3.2.2.4 Secondary effects of security solutions

There is the challenge to find a balance between **freedom and security**. The security should be good enough, so that we have low risks. If we have too much regulations, hackers will be motivated to find a way around it and organizations like Anonymous will then start to create problems. If millions of people in Facebook get angry about security regulations, the society will also get a problem.

Another interviewee thinks that it is more a problem of security on the one side and tremendous investments (**financial limits**) on the other side. However, if vulnerabilities are tackled head-on, the consumer faith in the stability of applications/devices/services will grow. This could represent a business opportunity in itself.

The **privacy** question is relevant to mobile applications. Can the end-user trust that the data is secure? The responsibility for privacy issues lies primarily with the product developer, but the government can of course take on an active role.

3.2.3 Environmental issues

In this chapter the following reports with the focus on threats, needs and/or security solutions were exploited: European Security in Light of Evolving Trends, Drives and Threats – FORESEC and Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles – FOCUS. The results were combined with eight interviews already completed in the area of environmental issues.

3.2.3.1 Threats

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

In the FOCUS project the hazards were divided into "**high system level hazards**" (like climate change) and the "**classic" natural hazards** (like flooding or volcanoes).[20] The high system level hazards rarely constitute a direct security problem, but they lay the scene for many of the "classic" hazards – triggering them, enhancing their probability of occurrence and amplifying their intensity or their effects.[20] Although measures to prevent and mitigate the *natural hazards* themselves are necessary and useful, there are not sufficient. The problem is that the underlying developments at a *high system level* evolve to trigger increasingly larger catastrophes.[20] Thus the hazards on the high system level are in essence a security issue and must be addressed with high priority.[20]

[20] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

High system level Hazards

Climate Change	Stratospheric Ozone Depletion	Change in Land Use
Biodiversity Loss	Ocean Acidification	Increase in Atmospheric Aerosol Loading
Changes in the Biogeochemical Flow	Increase of Global Freshwater Use	

Table 5 - High System Level Hazards. Taken from the map of vulnerabilities of the FOCUS project. Source: FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

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

Impacts of climate change in a ten years perspective is not a big threat, but after that it is. One risk associated with climate change is new migration patterns. Another risk is that climate change could increase imbalances within the EU, especially between the North and the South.

Climate change is also seen as the driver for a series of consequences like sea-level rise, glaciers melt, crop shortfalls, change of Gulf Stream, spread of tropical diseases, loss of biodiversity, migration, and so on.

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

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

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

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

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

One interviewee sees a threat in the **commercialisation of the ecosystem**. Although ecosystem services is an important concept that might be part of a solution to environmental problems, but there are also risks if we are putting "a price on the environment".

"Classical"/ Natural hazards

Earthquake	Sea-Level Rise	Dust & Sand Storm
Mass Movements (avalanche, land slide, slope failure, cave collapse, sinkholes, subsidence, etc.)	Flooding	Earth Axis Rotation Aberration
Volcanoes	Wildfire	El Nino
Tsunami	Extreme Weather Events	Famine
Impact of Space Objects	Flash Floods	Geomagnetic Storm
Heat Wave	Tropical Cyclones	Lightning
Pan/Epidemic (humans)	Plant Diseases	Seiche
Droughts and Desertification	Permafrost Thawing	Solar flair

Table 6 - Natural hazards. Taken from the map of vulnerabilities of the FOCUS project.
Source: FOCUS, Problem space report: Natural disasters and global environmental change, Deliverable 4.1, Jan. 2012.

The EU project FORESEC investigated the impact of extreme environmental events on the European security.[21] These events were divided into geophysical or tectonic events and weather or climatic events.[21]

- *Tectonic events:*

  In Europe major hazards which pose a threat to densely populated areas are earthquakes, **volcanic fields** and offshore earthquakes, which may trigger submarine landslides and tsunamis.[22] In high Alpine areas, thawing of permafrost increases the danger from gravitational **mass movements**, partly triggered by earthquakes.[22]

  It is statistically likely that Turkey and Iran will again experience large and **damaging quakes** between now and 2025, and it would not be surprising for such events to occur in

[21] FORESEC, Report on European Security: Trends, Drivers, Threats, Deliverable D 4.5, Aug. 2009.
[22] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

Italy, south-eastern Europe (including Greece and its islands), North Africa or the Caucasus.[23] Great quakes of magnitude over 8.0 cannot be ruled out in any of these regions, particularly Turkey or Iran.[23]

- *Climatic events:*

The impacts of **heat waves** like in summer 2003 were severe: total EU wheat production fell by 10%, transport systems were disrupted, power plants were forced to shut down and there were an estimated 35,000 excess death.[23] Increased temperatures also foster **wildfires**, which lead to significant economic, social and environmental damage.[24]

Desertification of land can be nature driven or anthropogenic driven or a combination of both.[24] The drought at the Horn of Africa affects more than 13 million people, making them dependent on humanitarian assistance.[24]

The reverse of heat wave is the **cold snap**. Even in countries where society has adapted to routinely low winter temperatures, cold snaps can cause disruption and health impacts.[23]

Even more than half of all persons killed in the wake of natural disasters over the last decades lost their lives in **flood** events.[24] International studies highlighted, that the number of floods in Europe has dramatically increased at the beginning of the new millennium.[24] Secondary effects during and after floods concern water supplies (contamination of water), diseases due to unhygienic conditions, lack of food supplies and destruction of transport links.[24]

Storms in Europe consist of extreme, near-surface damage-causing winds (> 70 km/h).[24] Heavy precipitation in form of rain, snow or hail as well as lightening can be part of the storm.[24] The storms in recent years caused considerable wind damage to transport, forestry and energy infrastructures while crossing Europe.[24]

There are also cyclical weather patterns on various timescales which are subject to variations in timing and severity, too.[23] The most important of these is a 2-7-year cycle of fluctuation in the **El Niño** – Southern Oscillation (ENSO) system.[23]

There is also a potential for sudden, non-linear impacts such as **abrupt sea-level rise or regional cooling** through shut-down of warm ocean currents such as the Gulf Stream caused by the infusion of cold, fresh melt water from melting ice caps. These potential impacts are "abrupt" in the sense that they occur much faster than the underlying temperature that induce them.[23]

[23] FORESEC, Report on European Security: Trends, Drivers, Threats, Deliverable D 4.5, Aug. 2009.
[24] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

Natural hazards can also threaten **nuclear power plants**.[25] The Chernobyl and Fukushima accidents have shown which far reaching effects accidents at nuclear power plants can have.[25]

- *Biological Hazards:*

High intensity rearing of a small number of breeds and varieties of animals and plants produced in monocultures, combined with the relative ease of transportation within the EU, allow **diseases** and pests to spread rapidly and have high impacts on agriculture.[25] In addition, potential effects of a changing climate and GM technologies bring unknown biological hazards.[25]

Concerning human health impacts, the most feared outcome of communicable diseases are **epidemics** and pandemics (e.g. HIV/AIDS, potentially: influenza).[25]

- *Environmental pollution:*

Environmental pollution can occur in various forms: **water-, air-, soil- and sound pollution**. When dangers arise to public health, this is often at a local level. In large parts of the world this can lead to potential social unrest. Large scale environmental pollution can lead to diseases or to soil pollution/degradation which reduces the arable land.

One Interviewee sees the biggest threat in his area in **chemical accidents** – both inside industrial companies as well as during transport of hazardous materials. The expert is worried about a situation getting out of hands when the hazardous material is widely spread and a large number of persons have to be evacuated.

Another interviewee is especially worried about environmental pollution due to excess unreacted nitrogen compounds entering the environment. In the agriculture we are using multiple times the amount of **nitrogen** naturally introduced to the soil. Additionally we have the problem of too much nitrogen compounds in waste water.

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

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

[25] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

- *Meteorite impact:*

Explosions in the earth's atmosphere of **space objects** and impacts of such objects on earth can result in damage to facilities and infrastructures from direct and indirect causes.[26]

1. Hurricanes	1. Flooding
2. Sturm surge	2. Avalanches
3. Flooding	3. Other natural disasters
4. Snow drifts (collapsing roofs due to the snow load)	4. Power blackout
5. Heat waves (water scarcity)	5. Pandemics
6. Interruptions of supply change	6. Accidents releasing radioactivity (Fukushima)
7. Oil leakages (on the coast)	
8. CBRN accidents or attacks	
9. Earthquakes (especially in Istanbul	
10. Tsunami in the Mediterranean	
11. Impact of natural hazards on critical infrastructur	

Table 7 - Important scenarios in the area of environmental threats (from two different interviewees).

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

One interviewee thinks that perhaps in Northwest Europe and the US and perhaps even in China the society will have enough innovative capacity to **adapt sufficiently to the pace of developments** (population growth, need for energy, food and water). But many less developed countries and regions in the world will face difficulties.

Another interviewee also thinks that in the next 15 to 20 years Europe will not undergo serious societal changes due to environmental threats. On the other side in poorer regions of the world, the climate change will probably lead to famine in this period of time.

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

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

[26] FOCUS, Problem space report, Critical space infrastructure & supply chain protection, D 5.1, Jan. 2012.

3.2.3.2 Societal Needs

Within the European Union there is a need to **spread the knowledge** about climate change and its consequences. The society should develop a deeper understanding of the underlying problem.

Additionally the society should be **educated** how to live with the consequences of climate change – how to behave in hot summers and how to protect themselves in flood areas.

It is more difficult to educate the society outside Europe, as every small region might have its own problems regarding climate change. So it is necessary to provide all the specific information for this local area and include also the traditional knowledge of the local people. The problem is that in many cases the local population does not have the (financial) resources to accomplish the adaption process to climate change on its own. So in these cases they have to rely on international help.

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

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

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

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

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

3.2.3.3 Solutions

Several interviewees mentioned that we should promote the **resilience** of the society. We should provide trainings and programmes so that the people are better able to help themselves in case of an emergency. Also **knowledge and education** about climate change were seen as key issues.

We should learn more about **decision science**, what motivates people, what makes people change. It is not sufficient to have the technological solutions; we also have to understand what makes people accept the change (e.g. incandescent light bulbs in EU; difference of energy consumption in EU and USA).

We also need better **warning systems**. At the moment we do not have a good warning system to be able to evacuate a city of one million people. One interviewee suggests intensifying research in the area of the usage of smartphones as part of the warning system.

It is also seen as important to promote international **networks** of experts and end-users and to make sure that these networks are not dominated by national views. We should also try to cooperate outside the "comfort zone", i.e. do not only cooperate with likeminded western nations.

One interviewee said that we need better capabilities in the area of **logistics** and infrastructure (energy, telecommunication, water, administration). For example we should be able to provide the citizens with an extensive electricity supply in case of an emergency.

Another important area is **communication**. We should be able to sustain at least the communication of the crisis management team (authorities, civil defence, military) in a scenario with a power blackout of several days.

We should invest in better capabilities in the area of **reconnaissance**, search and rescue of people as well as technologies for indoor localization and transmission of vital signs.

Energy issues were mentioned by several interviewees as key to sustainability and security. An important part is the energy turnaround to include more renewable energies in our system as well as research in better energy storage technologies.

One of the interviewees said that it would be very helpful if plants and food crops would grow with less water and energy. That would make our **food system** more resilient. It will also be of great value, if we manage to convert seawater into drinking water at a low cost and a lower energy usage.

Gene technology and nanotechnology are seen as promising areas by one of the interviewees. It was said that these technologies should be pursued to help us solve our problems.

3.2.3.4 Secondary effects of security solutions

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

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

4 INPUT II: WEAK SIGNAL MINING

4.1 INTRODUCTION

Finding potential new threats on the internet is notoriously difficult for an automated scanning process. Humans usually use semantic judgements to decide whether there is a threat in an internet discussion or not. Whether this threat is new, emerging or of declining importance is even more difficult for humans to find out. Therefore we will not try to copy the human approach but use statistics to identify potential new threats. The method is described in detail in chapter 4.1.2. Despite the number of reasons why automatic scanning is a problematic approach, there is at least one very good reason to start with an automatic approach. The amount of content has increased exponentially in the last decade and it is foreseeable that this trend will be stable in the next decade. Therefore, it is important to develop methods for threat identification which scale well on large data sets.

4.1.1 Objectives

The main goal of the text mining in WP4.2 is to identify possible future threats on the internet. As "future threats" are a very abstract concept it is not possible to search these threats with a simple semantic search strategy. Consequently a two-step search strategy was developed. In a first step a community was identified; in which members of the community publish content about future threats on the internet. In a second step, the content was clustered to find out about the main topics of possible future threats. Following this, an in-depth analysis of these identified topics was conducted to get hints about possible weak signals for future threats.

4.1.2 Approach

The "future threats" community on the internet can be seen as a kind of epistemic community in a sense that members of the community cooperate in knowledge generation for their personal interest, their organization, their community or a wider public. Even if there is no formal membership most of the community members have similar interests, related to knowledge generation, knowledge distribution and knowledge preservation.

In general scanning the WWW for identification of epistemic groups is a resource-intensive and expensive task. Google indexes about 1.3 trillion sites with approximately 20 trillion links. For our purpose it is obviously not a cost effective idea just to crawl the web and set up a social network analysis on these results. There are basically two ways to find out what content about future threats is visible on the WWW:

The first possible way is to use all the statistics and the tools that are available for searching the Web, which are Google Trends, Alexa, and other similar tools.

Another possible way is to use site statistics and social network analysis to identify the community. In our approach we developed a software to identify relevant sites and from there went on to the next linked sites, checking whether these sites have content relevant to future threats, and collected all necessary data from the relevant sites.

Both ways have advantages and disadvantages. On one hand Google results are easily accessible and resource effective. On the other hand Google does not provide much information about how these results were received and whether they are reliable or not. The main disadvantage is, however, that Google's results are cut off after 1000 sites. So it is not possible to identify all sites from a community. In order to identify and download the sites from the "threat" community on the internet we used a combination of both approaches in this project.

As the Google search statistics is straight forward and easy to understand we will concentrate on site statistics and web crawling in this methodical discussion. One starting point for the engineering process in ETTIS 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 the threat identification agent (TIA) was developed by Joachim Klerx, AIT. The following Figure 6 gives an overview of the overall system architecture of the TIA.

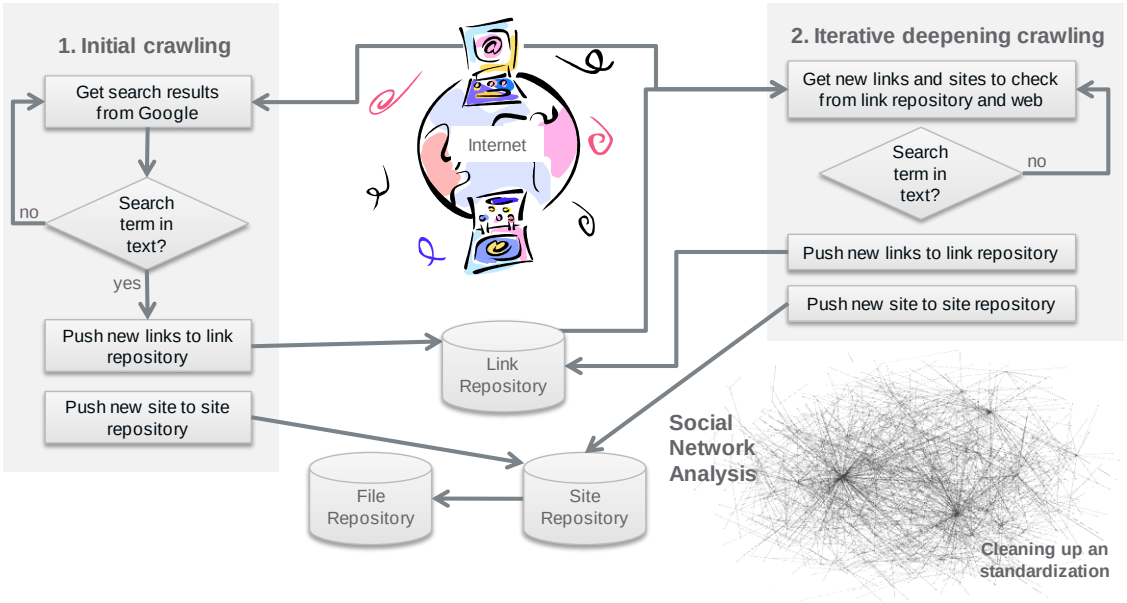


Figure 6 - System architecture of TIA agent v0.1.
Source: AIT

In the initial crawling stage the agent loads search results from a search engine like Google, which are considered as relevant for the search conducted, in our case 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. In the case that 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 "black holes"[27] 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.

Based on this 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 about 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 analysed to identify possible weak signals.

4.1.3 Search strategy for society threats

It is crucial for the whole threat identification process to have a relevant dataset. Relevant means that only sites containing the topic are in the data set and that almost all sites available on the internet are in the data set. Therefore some analytical considerations were conducted to identify a search strategy that covers almost all of the relevant sites and leave out irrelevant sites. The following table summarizes the results that can be expected from different search strategies for the threat identification process and discusses relevance measures for this.

[27]Stackoverflow.com, "What techniques can be used to detect so called "black holes" (a spider trap) when creating a web crawler?", http://stackoverflow.com/questions/4512936/what-techniques-can-be-used-to-detect-so-called-black-holes-a-spider-trap-wh

Google indexes almost all sites on the internet and it offers a kind of search statistics on his result list. This can be used to get an educated guess of what can be expected, by using a specific search strategy for crawling. Even if the total number of sites is usually much too high (because of black hole sites and false positive sites for technical reason), it gives some hints to the size of a community. The first 100 search results from Google offer some clues about the quality of the results. In the following table different possible search strategies for potential future threats are compared against each other to identify the best search strategy for the TIA.

id	Query	Google	Relevance
1	threats	154,000,000	basis
2	emerging	210,000,000	basis
3	future	2,170,000,000	basis
4	emerging threats	5,220,000	not a topic
5	"emerging threats"	1,200,000	relevant topic
6	"emerging threats" security planning	363,000	highly relevant
7	"emerging threats" capability planning	1,280,000	other topic
8	"emerging threats" "capability planning"	713	subtopic
9	"emerging threats" research agenda	33,800	subtopic
10	"emerging threats" foresight	48,700	subtopic
11	"emerging threats" security politics	270,000	highly relevant
12	"emerging threats" research	512,000	relevant topic
13	future threats	153,000,000	not a topic
14	"future threats"	518,000	highly relevant
15	"future threats" security planning	168,000	subtopic
16	"future threats" security politics	550,000	highly relevant
17	"future security threats"	332,000	subtopic
18	"future disaster"	168,000	subtopic
19	"future crisis"	175,000	subtopic
20	"cyber threats"	2,070,000	other topic
21	"nuclear threats"	438,000	other topic
22	"environmental threats"	715,000	other topic
23	"European Security"	1,340,000	other topic
24	"European Security" threats	511,000	highly relevant
25	"security threats"	7,220,000	relevant topic
26	"cyber weapon" emerging future	113,000	subtopic of cyber secutity
27	Europeas "amenazas de seguridad"	1,370,000	Topic in Spanish language, translation ?

28	"Européennes de sécurité" menaces	39,100	Topic in French language
29	"Europäische Sicherheit" Bedrohungen	33,600	Topic in German language
30	"Europees veiligheids" bedreigingen	10,400	Topic in Dutch language
31	"欧洲安全的”威胁"	1,250,000	Topic in Chinese language
32	"出版バイアス"	952,000	Topic in Japanese language

Table 8 - Statistical review of possible search strategies for “future threats”.
Source: AIT

Considering the quality and quantity of search results the best search strategy seems to be “future threats” as a string. Therefore, this will be used in the first crawling process with TIA.

In addition to the indexing statistics, Google provides some basic data about the quantity of searches, for words and word combination. We made use of this information to find out whether we operated with the appropriate terms. Google Trend data point to the direction, that crisis and disaster are statistically very similar to threats. The following graphic shows the relative quantity of searches for threats (in green, not visible, because of the low amount of searches), disaster (orange), crisis (red), and security (blue), as an overall concept, over the last few years.

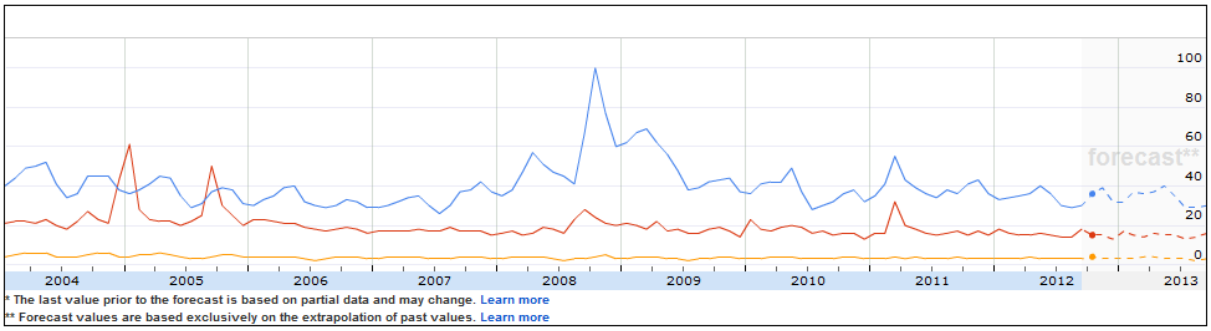


Figure 7 - Amount of relative searches for the term “threat” and synonyms.
Source: AIT, Google.

Disaster and crisis are used in searches, when an event happens. Thus there is some systematic bias, caused by actual events for the word crisis and disaster. Threat is used as an abstract term for a potential crisis or disaster. Thus, threat for us is a more specific term, to what we are looking for.

The geographic distribution of crisis and disaster (as visible in the annex) supports the theory, that these words are used mainly in a corresponding context to an actual threat event. Crisis is

very often used in the context of economic crisis and in areas, where an economic crisis takes place. The term disaster is used, when a natural or manmade disaster takes place. Threat and security are more abstract terms, which are used in English speaking countries.

The following figure shows a slightly declining amount of searches with the term “threat”, for Google searches worldwide. Thus the threat discussion worldwide is not an emerging issue.

Figure 8 - Quantity of searches, with the term “threat”.
Source: AIT, Google.

However the geographic distribution of search requests for “threat” shows that there is a remarkable interest for “threats” in countries with a remarkable number of problems, like poverty, economic crises, social unrest corruption or civil war.

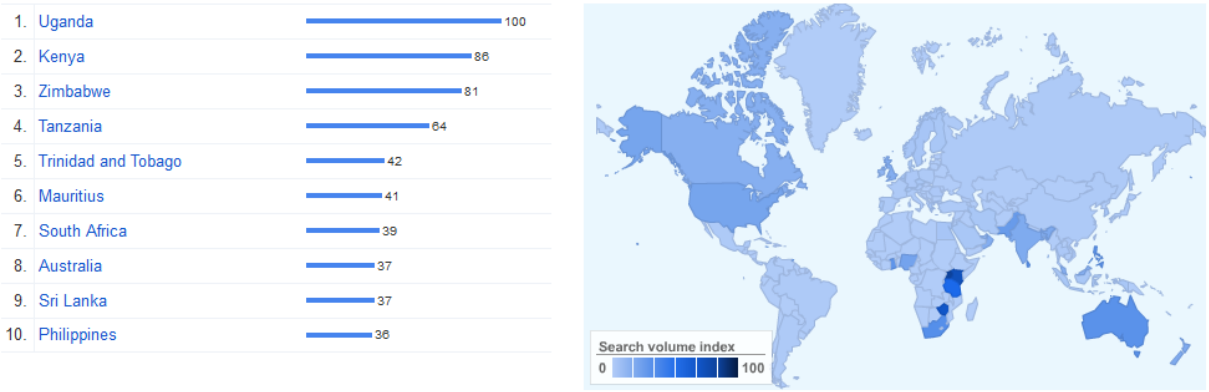


Figure 9 - Geographic distribution of searches containing the term “threat”.
Source: AIT, Google.

Countries like Uganda, Kenya and Zimbabwe face different threats at the same time and thus people from these countries uses more Google searches with the term threat in the search strategy.

Looking for rising topics from similar searches gives the first hint to emerging topics near by the discussion about threats.

Top searches		Rising searches	
1. the threats	100	1. facebook threats	Breakout
2. security threats	40	2. malware threats	Breakout
3. death threats	35	3. obama threats	Breakout
4. threat	25	4. cyber threats	+180%
5. swot threats	15	5. death threats	+120%
6. bomb threats	15	6. threats to data	+100%
7. swot	15	7. biodiversity	+60%
8. virus threats	15	8. it threats	+60%
9. computer threats	10	9. internal validity	+50%
10. opportunities and threats	10	10. bomb threats	+40%

Table 9 - Rising topics, similar to "threats". Source: AIT, Google.

Topics like Facebook threats, malware threats, and cyber threats indicate that cyber threats are an emerging issue at the moment. As biodiversity is also mentioned as rising search with about 60% increase, this is a first hint for another possible future threat topic.

To summarize the discussion above it can be stated that:

- "future threats" is a good search term for automatic threat identification with TIA;
- cyber threats, bio threats and bomb threats are maybe topics for in depth analysis;
- threat discussion on the internet seems to be context dependent, so that the discussion intensity increases around a threat event and decreases if no threat is realized.

The main drawback from Google search statistics is that absolute figures are not published by Google. In addition, Google has an unspecified number of manual changes in the search index and in their statistical figures, to improve the search results from Google (in a way, Google expects, that the user of their search engine would like to have the search results. The automatic internet crawling with TIA is more neutral. It has the potential to overcome these drawbacks and give a better quantification of the discussions in the threat community.

4.2 RESULTS OF SCANNING FOR FUTURE THREATS

As described in the methods chapter 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 expression of trust from the link source site to the 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, whereas an authority node is a site with a lot of inbound links and a hub is a site with a lot of out bound links.

The agent identified about 80,000 links in sites containing the phrase "future threats". From these links all were checked against the search strategy of TIA, by downloading the site,

parsing the html and check whether the term “future threats” was in this text. About 6,000 sites were identified.

The following network figure shows two types of network structure of internet sites. On the left side is a typical high integrated network of an epistemic community. TIA discovered that the “future threats” network looks like the symbolical network on the right side.

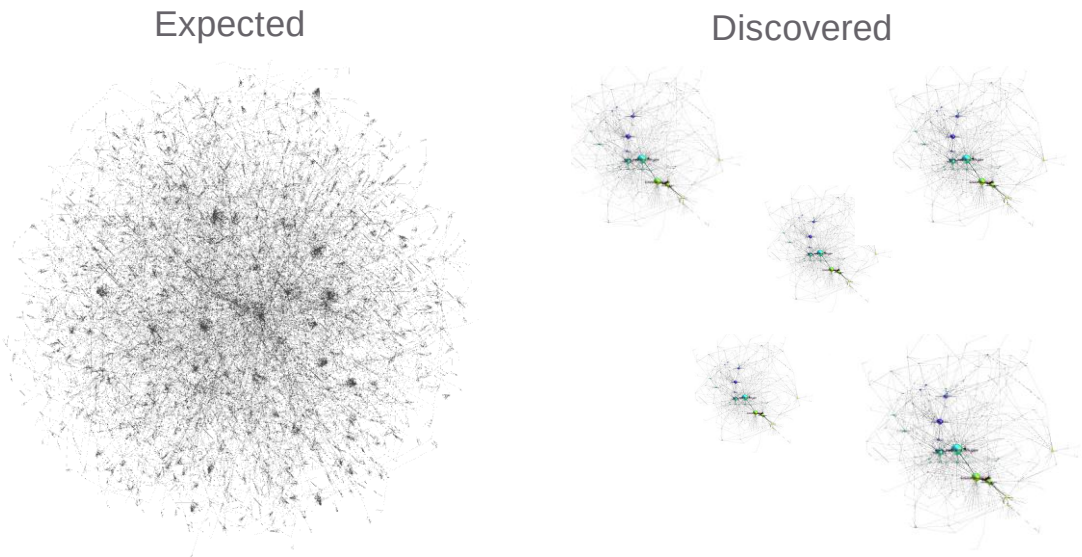


Figure 10 - Network structure of the TIA results (symbolic).
Source: AIT

The average site in the integrated network has about 15 links to other relevant sites, in a way, that each node is integrated in the network. A small amount of sites has a much larger amount of inbound and outbound links. The discovered network however consists of an unknown number of subnets. These networks are typically topic specific and are not connected to subnets with other topics. This is obviously caused by the wide range of different threat contexts. The problem with this is that it is not easy to download all sites from the network, as it is difficult to get access to a site, if the link is not known. Every time the crawler stops, because of a shortage of links to new sites, it is necessary to provide some links to a new subnet manually. Therefore a new crawling strategy will be implemented for the next crawling round.

Nevertheless it was possible to conduct a cluster identification. The following figure shows the results. These results should be interpreted keeping in mind that important thematic subnets might be missing. However in the next round of crawling this will be improved.

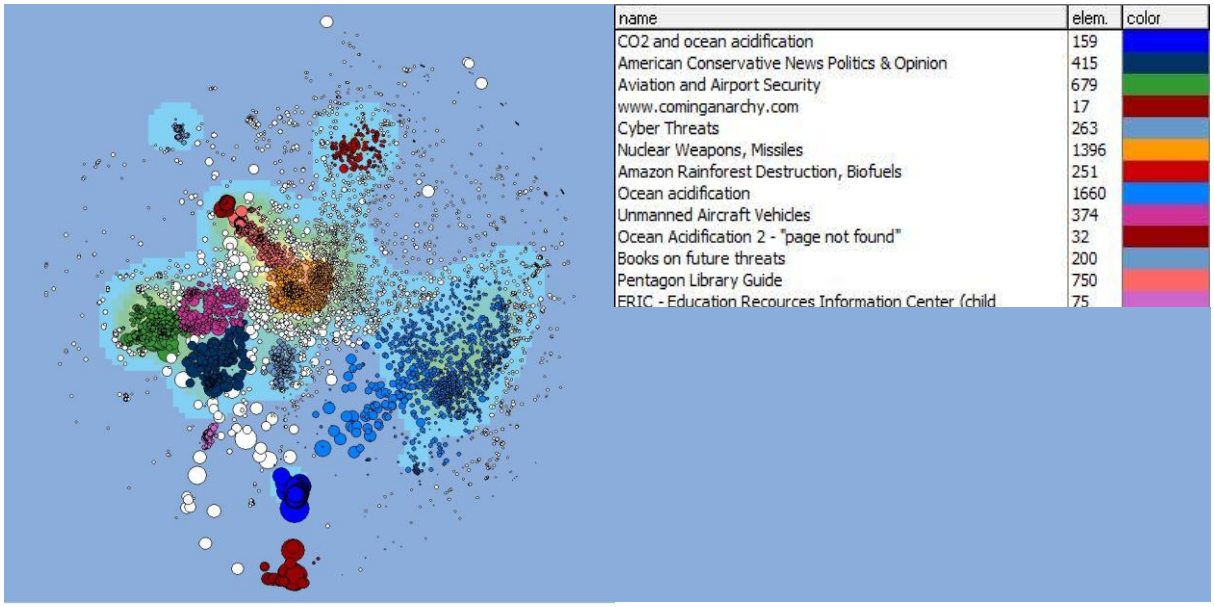


Figure 11 - Results from topic identification.
Source: AIT.

For the time being cyber threats, nuclear threats, political threats, natural and environmental threats have been identified as important topics in the threats discussion.

Having the results from ETTIS WP 2, 3 and 4 in mind, the following topical subjects:

- cyber threats,
- nuclear threats
- and environmental threats

will be analysed in more detail.

4.2.1 In detail results for the subject "cyber threats"

As already discussed in Chapter 4.1, Google offers tools to access their statistics information about search pattern and search behaviour. We used Google Trends and Google Insights to check, whether identified topics are weak signals for emerging future threats. For interpretation of the following results, it is very important to have the differences between the threat identification with site statistics and the threat identification with search statistics in mind.

Site statistics use measurements from internet sites to identify possible future threats, whereas search statistics use measurements from the search pattern to identify pattern for weak signals.[28]

[28] Google, "How is the data scaled?", http://support.google.com/trends/bin/answer.py?hl=en&answer=87282&ctx=cb&src=cb&cbid=1vvr8ubxsfldt

The search statistics is a very volatile indicator for the "interest in the topic" over time. The next figure indicates that in 2007 a new public awareness concerning cyber threats arose.

Figure 12 - Quantity of searches, with the term "cyber threats".
Source: AIT, Google.

From then on, the number of searches for "cyber threats" increased slightly, but steadily until the present. A forecast by trend extrapolation shows that the search pattern is expected to remain stable, but volatile over the next years. Therefore, the topical subject can be seen as an emerging issue.

However the geographic distribution indicates that the search interest in this topic comes mainly from USA. For better understanding it is important to mention, that searches in this statistic are translated and equally counted, so that the results are language neutral.

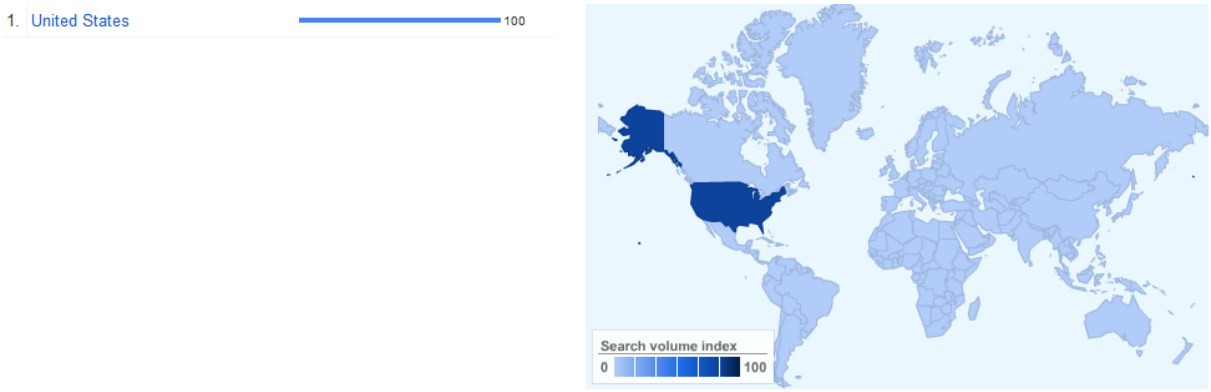


Figure 13 - Geographic distribution of searches for "cyber threats".
Source: AIT, Google.

Today cyber security is often used as a synonym for internet security or for computer security. The following Figure 14 shows, that internet security is historically the older term and probably used in a wider context. Thus there is not an increasing trend visible for internet security.

Figure 14 - Quantity of searches, with the term "internet security".
Source: AIT, Google.

The hypothesis that 'internet security' is a worldwide more common term for cyber security is supported by the geographic distribution of searches for "internet security", as visualised in the following figure.

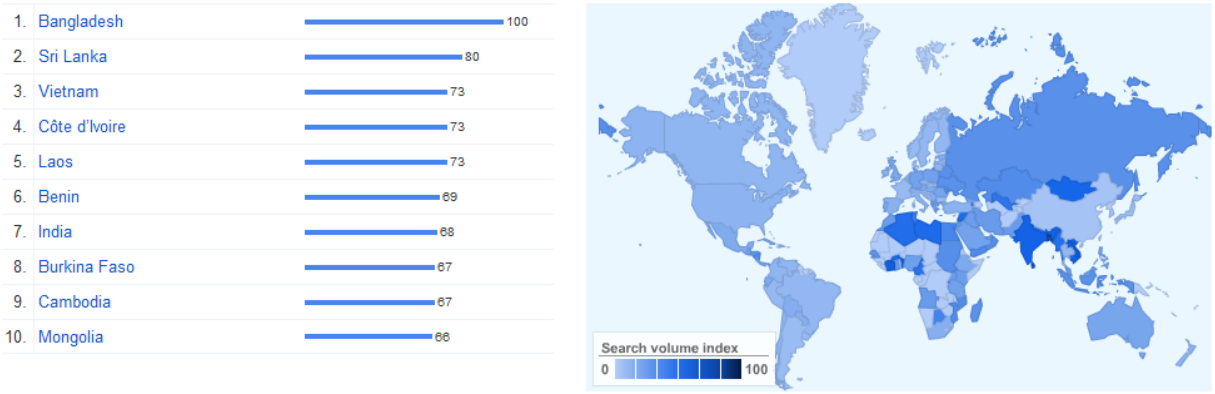


Figure 15 - Geographic distribution of searches for "internet security".
Source: AIT, Google.

A wide range of countries well known in the ICT security community are shown on this map. The trend from Figure 15 however implies, that "internet security" is not an emerging topic, but a topical subject (too large for a topic).

Inside the topical subject "cyber security" or "internet security" are a number of terms in the crawling results, which might be a weak signal for future threats, or at least might be an emerging issue. Black hat hacker, e.g. is a term, which is more intensely used in searches from the end of 2005 on.

Figure 16 - Quantity of searches, with the term "black hat" hacker.
Source: AIT, Google.

At the end of 2004 was a first peak in search uses, which might be more an insider hype. However starting from 2005 on, the term got a wider publicity.

Other terms with a certain potential for weak signals are mentioned in the following table. To be suitable for a weak signal, the term must not only be used more frequently in the last years, more important is that the term concept should point to a structural change or a game changing event. Therefore the final classification needs other methods to validate the weak signal property. The following table only summarizes potential weak signals on the basis of the web crawling method and thus is not a final judgment.

For the topical subject it was very easy to find a lot of technical details about threats, needs and techniques on the internet. For this topic a second crawl seems to be promising.

id	Query	Google	Weak signal potential
1	"cyber threats"	2,070,000	low
2	"computer security"	20,100,000	low
3	"internet security"	98,100,000	low
4	"information security"	30,900,000	low
5	"IT security"	15,400,000	low
6	"organized crime"	17,600,000	high
7	warez	131,000,000	medium
8	"botnet"	6,540,000	high
9	"trojan horse" computing	540,000	high
10	"trojan horse"	8,140,000	high
11	"trojan horse" virus	9,620,000	high
12	"computer virus"	6,710,000	high
13	"computer worm"	505,000	high
14	"reverse engineering"	9,530,000	low
15	"stuxnet"	5,250,000	high
16	"zero days" exploit	58,800	high

17	"0-day exploit market"	27	high
18	"0-Day Exploit"	1,040,000	high
19	"zero days" attack	69,500	high
20	"Zero-day attack"	927,000	high
21	"denial of service attack"	1,300,000	high
22	"DoS attack"	1,620,000	high
23	"Smurf attack"	81,300	high
24	"arp poisoning attack"	72,400	high
25	"sql injection attack"	253,000	high
26	Metasploit	2,840,000	high
27	exploit "black market"	1,170,000	high
28	"black hat" hacker	1,520,000	medium
29	"cyber attack"	2,580,000	medium
30	"cyber warfare"	1,660,000	high
31	"future cyberwarfare"	1,680	high
32	"future cyber warfare"	333,000	high
33	"cyber terrorism"	828,000	high
34	"future cyber terrorism"	59	high
35	"cyber weapon"	309,000	high
36	"cyber weapon" -flame	174,000	high
37	"cyber weapon" emerging future	113,000	high
38	Sykipot	41,100	high
39	"Elderwood platform"	6,240	high
40	"cyber espionage"	530,000	medium
41	"Aurora Trojan"	18,200	high

Table 10 - Overview about topics for potential weak signals in "cyber threats". Source: AIT

4.2.2 In detail results for the subject "nuclear threats"

The crawling results in detail resulted only in well-known strategy documents for nuclear power, nuclear safety or nuclear research in general. Therefore, we use Google search indexing to find out about the basic structure of the subject "nuclear threats" and whether potential weak signals are in our data set.

The following figure shows the Google trends index for the subject "nuclear threats". It is an interesting fact that there was a strong increase and decline of searches for nuclear threats in 2005 and again in 2006.

Figure 17 - Quantity of searches, with the term "nuclear threats".
Source: AIT, Google.

The geographic distribution shows, that there are a lot of searches from USA, looking for nuclear threats.

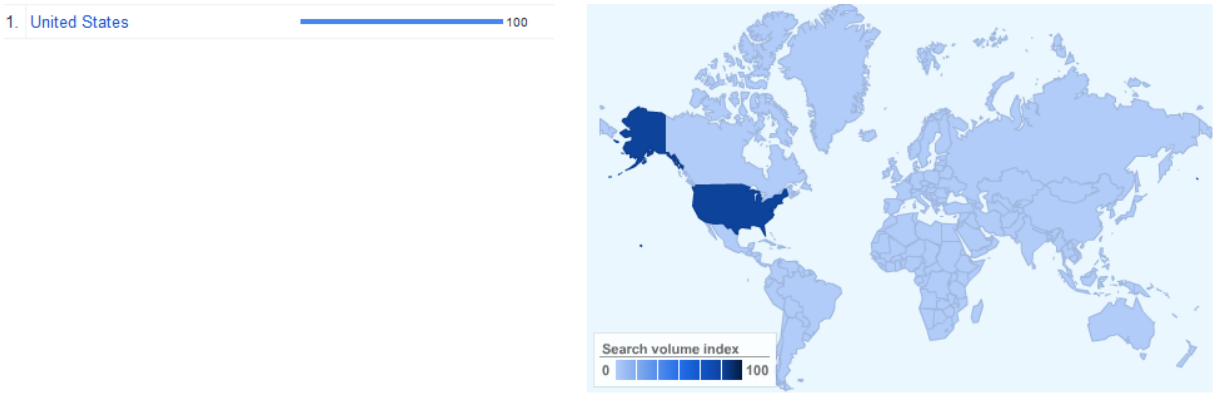


Figure 18 - Geographic distribution of searches for "nuclear threats".
Source: AIT, Google.

The large number of USA located searches suggests, that there are other word combinations used from other countries to address this subject. An obvious search strategy close to nuclear threat might be the search term nuclear bomb.

The following Figure 19 shows the 9 year trend for searches about nuclear bombs. An interesting pattern of this search index is that it is declining over the last 9 years, with two peaks in 2006 and 2011.

Figure 19 - Quantity of searches, with the term "nuclear bomb".
Source: AIT, Google.

The geographic distribution of searches for "nuclear bomb" shows searches in different nuclear power countries and countries struggling for nuclear power.

1.	United States	100
2.	Philippines	84
3.	New Zealand	82
4.	Australia	79
5.	Canada	78
6.	India	74
7.	United Kingdom	71
8.	Pakistan	70
9.	Singapore	69
10.	South Africa	65

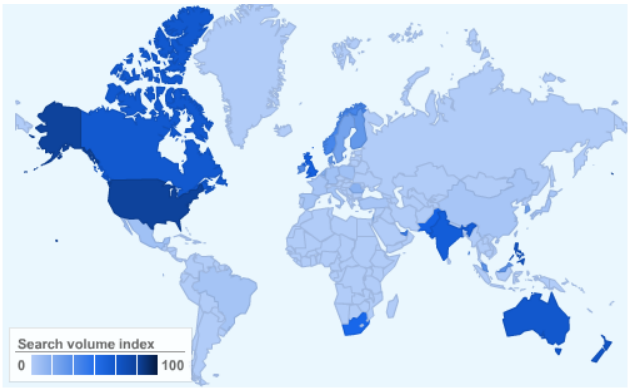


Figure 20 - Geographic distribution of searches for "nuclear bomb".
Source: AIT, Google.

To extend the search strategy top searches and rising searches of Google brings possible new search terms, as shown in the following table.

Top searches			Rising searches	
1.	the nuclear bomb	100	iran nuclear bomb	+200%
2.	atomic bomb	40	nuclear bomb radius	+200%
3.	hiroshima nuclear bomb	25	japan nuclear bomb	+160%
4.	nuclear war	25	biggest nuclear bomb	+130%
5.	hiroshima bomb	25	largest nuclear bomb	+100%
6.	japan nuclear bomb	25	nuclear bomb radiation	+90%
7.	nuclear bombs	20	the nuclear bomb	+70%
8.	nuclear bomb explosion	20	nuclear blast	+60%
9.	nuclear bomb video	20	first nuclear bomb	+50%
10.	nuclear weapons	20	nuclear bomb blast	+40%

Table 11 - Rising topics, similar to "nuclear bomb".
Source: AIT, Google.

The most increasing search strategy, which is similar to “nuclear bomb” was “iran nuclear bomb”. The following trend figure shows searches for “iran nuclear” (bomb was not necessary to get this result).

Figure 21 - Quantity of searches, with the term “Iran nuclear”.
Source: AIT, Google.

Again there are peaks in 2006 and 2011, like in the search for nuclear bomb. Now it becomes obvious, that the searches for nuclear bomb are triggered by the struggling of the Iran to get the nuclear bomb. Around 2006 Iran started the nuclear research program. At the end of 2011 was a public discussion about finishing the research program with the capability for building a nuclear bomb. This shows how sensitive search indexes react on public issues, which is not always an advantage in searching for weak signals and emerging issues, as these are more abstract concepts of potential future threats, than events of real threats.

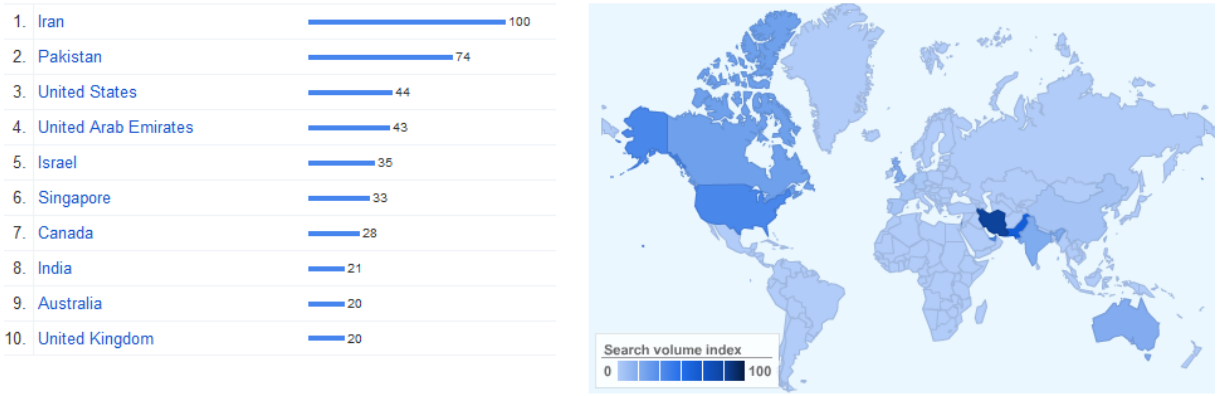


Figure 22 - Geographic distribution of searches for “Iran nuclear”.
Source: AIT, Google.

The geographic distribution shows, that besides Iran there is a high search volume for “iran nuclear” searches in Pakistan. Again, this is more driven by an actual event and not suitable for weak signal detection for new and upcoming threats, unless these new nuclear power countries might cause a shift in political power. This might cause new realized threats, but this is different to new future potential threats.

“Nuclear” as an even more general search term shows similar pattern. The following figure shows the search trend for “nuclear“.

Figure 23 - Quantity of searches, with the term “nuclear”.
Source: AIT, Google.

The most obvious pattern in this search trend is a peak in early 2011. According to Wikipedia, the Fukushima I Nuclear Power Plant did break down, following the Tōhoku earthquake and tsunami on 11 March 2011. Again, this is more an actual event and not a pattern for a potential future threat. However this threat was a signal for the German government to change their energy policy fundamentally.

To summarize the discussion, the following table shows potential weak signals for future nuclear threats. As mentioned in the text, the topical subject nuclear threat is not so well represented on the internet as cyber threats. One reason for this might be, that nuclear is not a new research field and some of the technologies seem to be mature. However the most probable reason for this seems to be that the nuclear threat community does not use the internet as main communication channel.

id	Query	Google	Weak signal potential
1	"nuclear threats"	438,000	low
2	"nuclear security"	2,780,000	low
3	"nuclear bomb"	5,960,000	medium
4	"Nuclear weapon"	6,350,000	medium
5	"nuclear nuke"	59,900	medium
6	"Nuclear Blast"	6,640,000	low
7	"Iran nuclear"	9,140,000	medium
8	nuclear threats	5,690,000	low
9	nuclear	351,000,000	low
10	"nuclear plant"	9,870,000	medium
11	"nuclear plant" threats	4,200,000	medium
12	cyber threats nuclear power plant	356,000	high
13	"nuclear plant" hacked	779,000	high
14	"nuclear plant" hacked -game	225,000	high

15	"nuclear safety"	3,690,000	low
16	"future threats" nuclear	105,000	low
17	radioactive	44,500,000	low
18	"radioactive threats"	5,400	low
19	"nuclear terror"	169,000	high
20	"Nuclear-armed terrorists"	766,000	high
21	"nuclear threat"	1,900,000	low
22	"nuclear threats" -iran	270,000	medium
23	"nuclear threats" -japan	358,000	medium
24	"nuclear wast"	4,310,000	high

Table 12 - Overview about topics for potential weak signals in "nuclear threats".
Source: AIT, Google.

4.2.3 In detail results for the subject "environmental threats"

The internet crawling for new threats has shown that there is not a single topical subject "environmental threats" on the internet. There are multiple topical subjects with own user groups and almost no communication between the groups, at least not via internet.

Google trends for the topic "environmental threats" show that searches for environmental threats are decreasing with high volatility over the last 9 years.

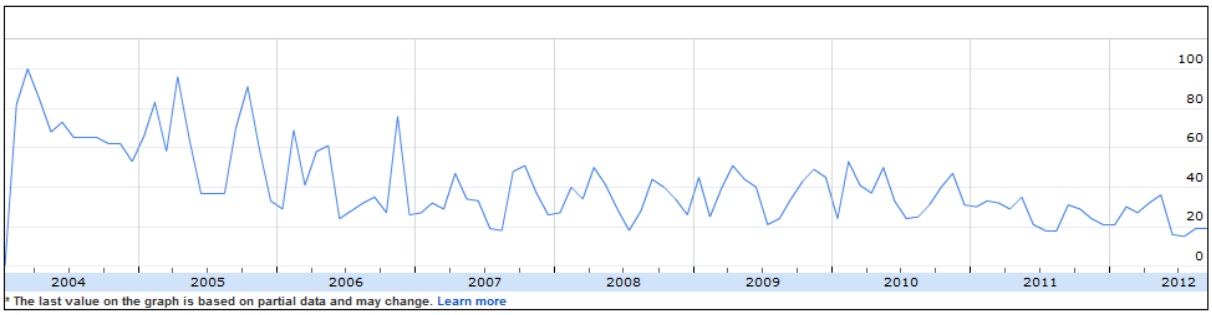


Figure 24 - Quantity of searches, with the term "environmental threats".
Source: AIT, Google.

The geographic distribution shows that USA and Australia are countries, where people are searching more for environmental threats.

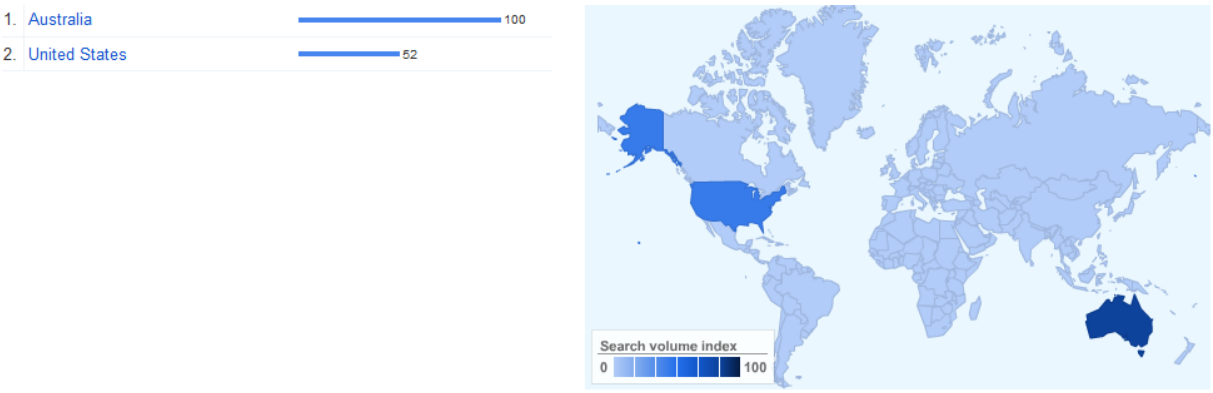


Figure 25 - Geographic distribution of searches for "environmental threats". Source: AIT, Google.

Given the fact, that most of the weak signals from internet crawling did not show some pattern for weak signal or emerging issue, these results were shifted to the attachment. The most promising result was, that the search term "extreme weather events" shows weak signal pattern.

Figure 26 - Quantity of searches, with the term "extreme weather events". Source: AIT, Google.

In the middle and at the end of 2005 were two preliminary peaks probably from experts, or driven by specific events. From end 2006 on searches for "extreme weather events" are visible and slightly increasing until today. For insurance companies these events have a remarkable impact on their business concept, as the probability of natural disasters increases.

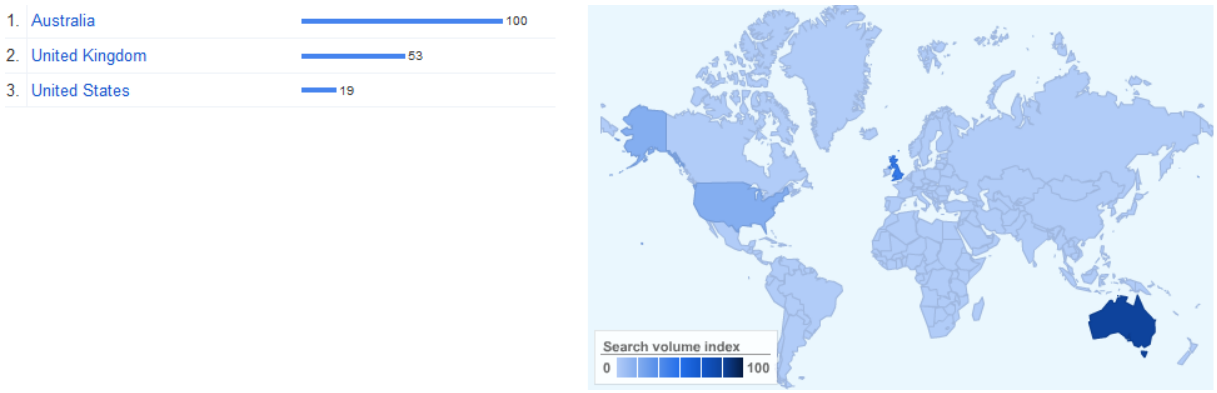


Figure 27 - Geographic distribution of searches for "extreme weather events". Source: AIT, Google.

The geographic distribution map shows, that these events are a public issue in English speaking countries.

Some additional statistical figures about potential future threats are in the appendix (as almost all of them did not show typical weak signal pattern). The in depth analysis has shown that the term "environmental threats" does not lead to a topical subject but that a bundle of different topical subjects is behind this term. Most of the topics we identified in the weak signal identification are actually topical subjects. Therefore it is necessary to look at these topics as a topical subject and to search inside these topical subjects for weak signals. This is probably the reason for the broken network structure. Each topical subject usually has its own network of experts.

As an example of this, we identified 4 different topical subjects about pollution (statistics is in the appendix):

- "water pollution"
- "air pollution"
- "light pollution"
- "noise pollution"

All of them are part of the "environmental pollution" and there is not only one environmental threat. This makes clear, that the term environmental threat is special and needs to be treated differently than cyber threats and nuclear threats.

id	Query	Google	Weak signal potential
1	"environmental threats"	715,000	low
2	"environmental threat"	415,000	low
3	"future threats" environment	250,000	low
4	environment	5,330,000,000	low
5	"novel pathogens"	19,100	high
6	"climate change"	115,000,000	medium
7	"extreme weather events"	1,570,000	high
8	deforestation	13,600,000	high
9	"global warming"	74,000,000	medium
10	Pollution	163,000,000	medium
11	"water Pollution"	11,300,000	high
12	"air pollution"	31,700,000	high
13	"light pollution"	2,460,000	high
14	"noise pollution"	4,560,000	high
15	"environmental pollution"	5,820,000	medium
16	"plastic trash"	1,190,000	high
17	"Loss of Biodiversity"	732,000	medium
18	"declining bee population"	96,000	high
19	"Melting Polar Ice-Caps"	477,000	medium
20	"Rising Sea Levels"	13,400,000	medium
21	"Oceanic Dead Zones"	120,000	high
22	"Explosive Population Growth"	1,340,000	high
23	"invasive species"	7,920,000	high
24	"genetical engineering"	8,980,000	high
25	"man made viruses"	78,100	high
26	"biomimetic robots"	28,500	high
27	"genetic engineering" threat	1,440,000	high
28	"food security"	21,800,000	medium
29	"genetic engineering" food	6,770,000	high
30	"Threats to Food Security"	337,000	high

Table 13 - Overview about topics for potential weak signals in "environmental threats". Source: AIT, Google.

4.3 CONCLUSION

To conclude the internet scanning could identify a number of potential weak signals, but has a fundamental methodical drawback, because of the heterogenic network structure. Because of this network structure we probably missed some important information, so that the list of potential weak signals for future threats is not extensive.

For some topics the internet as source for content is better than for other topics. For cyber security, e.g. there is a lot of very detailed threat information. For nuclear threats it seems, that some important information are missing or are only available in expert libraries. For environmental threats there is a huge amount of information about threats, on the internet. But this information is in different subnets and it needs a different crawling technique to get this information.

For the second crawling it is important to adapt the crawling strategy to deal with the heterogenic network structure problem and with the other problems mentioned.

5 SETTING THE FOCUS WITHIN THE DOMAINS

The domains cyber infrastructure, nuclear and environment are very broad and include many different issues. For the scenario development a concrete description of the content is necessary. On the basis of the following selection criteria one focal issue for each domain was selected:

- existing of available research work or data,
- results of the first phase of the interviews (task 4.1),
- the first interim findings of the weak signals mining (task 4.2),
- relevance for the EU (e.g. geographical, political),
- relevance for the stakeholder,
- relevance for institutions: public vs. private,
- focus on society.

The relevant issues, which are relevant for scenario development, result mostly from the findings of the desk research analysis of the future studies within the domains cyber infrastructure, nuclear and environment. Furthermore the findings of the WP2 (D.2.2), which deliver an analysis of a representative sample of projects illustrating several dimensions of security: physical, political, social, economic and cultural, environmental and radical uncertainty, cyber and information will be used.

The first results of the interviews with key stakeholders (chapter 3) as well as the weak signal mining (chapter 4) also debate these issues. Although they primarily provide information on the threats and needs, they were used for identifying the key factors and their future projections.

5.1 NUCLEAR

The findings of the desk research analysis of future studies related to the fields of nuclear material use are the following:

- nuclear power plants
- fuel cycle facilities
- research reactors
- radioactive waste disposal facilities
- mining and milling
- application of radiation sources
- transport of radioactive material

The findings of task 2.2 show a similar picture (see D.2.2).

Disruptions, attacks and accidents to critical infrastructures, intentional or accidental, perpetrated by states, terrorists criminals or radical groups
Transportation, energy, water and food supply, nuclear power plants, air-traffic control
Uncontrollable use of nuclear material (i.e. in Middle East)
Natural or man-made major disasters and accidents
Major technological disaster (e.g. nuclear accident)
Environmental degradation
Waste management risks and dumping of hazardous waste (e.g. nuclear waste, CCS facilities)

Table 14 - Findings from WP2 related to the domain nuclear.

The interviews showed that globally the stakeholders are worried about nuclear weapons – about the unlikely but still existing threat of the usage of nuclear weapons, but also about the storage and transport of nuclear weapon material. Within Europe the focus was more on potential terrorist attacks on nuclear power plants and about safe ways of handling and transporting nuclear materials, including from civilian sources like hospitals (see chapter 3.2.1). The results of weak signal scanning underlined the importance of threats to nuclear power plant as well as nuclear waste (see chapter 4.2.2).

Therefore we decided to emphasize the following aspects of nuclear security in the focus group workshop: nuclear power plants, use of nuclear material, nuclear accidents, waste management risks and dumping of hazardous waste.

5.2 CYBER INFRASTRUCTURE

The findings of the WP2 show that the EU-funded cyber security research gives priority to threats emerging from the privacy-cyber nexus and cybercrime (see D.2.2). The main reason for that is that cyber and information concerns are growing fast. This trend is mirrored in most recent projects and programmes. If modern, economically developed countries are increasingly becoming "information societies", then, it follows that threats to information are threats to the core of these societies. Security of private data and the growth of cybercrime are main perceived risks with regard to cyber-space and cyber-related activities. In addition, the risk of cyber attacks and sabotage, perpetrated by states, terrorists or individuals, is a dominant threat trend in several recent programmes. Finally, the increasing vulnerability of existing and new information technologies, both in relation to opening new opportunities for wrongdoings and weakening civil liberties or new individual rights (i.e. data privacy), is an important threat to state, society and individual.

The following table details the result of the clustering by key dimensions from task 2.2.

Spread of cyber attacks & sabotage perpetrated by states, terrorists or individuals
Memory attacks and exploitation techniques
Attacks on devices
Denial of service
Critical infrastructure attacks (e.g. airport information system attacks)
Social network and privacy attacks
Web service and applications attacks
Malicious hardware
Network-level attacks
Virtualization and cloud attacks
Information risks & espionage
Cyber and electronic warfare (including in outer space)
Spread of cyber crime (e.g. identity theft, online fraud, cyber-bullying, cyber-stalking, cyber trespass, cyber deceptions and thefts, cyber pornography, phishing, cyber-violence, data fraud and loss)
Increasing vulnerability of existing and new information technologies (e.g. openness and universal access, criminogenic)
Computer and internet of things
Mobile phones
RFID
Data storage and cloud computing
Artificial intelligence and cyborg technology
Technology for outer space

Table 15 - Result of the clustering by key dimensions within cyber security research from WP2

The findings of the desk research are the following (see Figure 28):

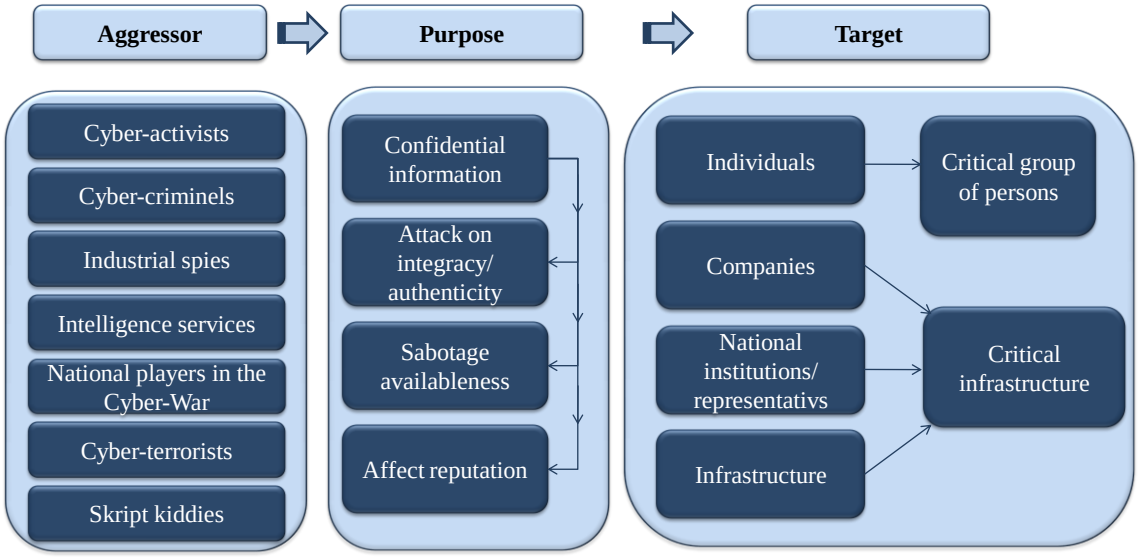


Figure 28 - Result of the desk research for exploring the domain cyber infrastructure (related to cyber attack).
Source: Bundesamt für Sicherheit in der Informationstechnik, "Register aktueller Cyber-Gefährdungen und –Angriffsformen", https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Gefaehrdungslage/Register/cs_Register_node.

The purpose considers such aspects like:

- Confidential information: direct monitoring (e.g. cable, radio, network), direct access (e.g. hotel, customs), burglary, shoulder surfing, recovery of deleted information
- Attack on integracy: manipulating of information (e.g. data medium, software, communication channel, interfaces or access points, special IT of security components)
- Attack on availableness: sabotage of information and IT services (e.g. denial of service attack, physical destruction, burglary)
- Attack on authenticity: attacks on the integrity include as a special case, attacks on the authenticity (e.g. the feigning of a false sender)
- Affect reputation: damage to the reputation of persons or institutions due to the aforementioned attacks

The interviews in the area of cyber security showed that in general the threats in the cyber world a getting more complex and that both the gravity of threats as well as the costs of the incidents are growing fast. It also can be observed that the trend is clearly moving in the direction of state or state-enabled actors and serious international crime. The type of threat covers a rather broad range from spam and phishing to serious crime like botnets and data breaches (see chapter 3.2.2). The weak signal scanning underlined the importance of serious criminal attacks like cyber warfare (see chapter 4.2.1).

The foregoing tasks have shown that in the focus group workshops we have to cover a broad range of cyber risks to get a clear and sufficiently complete picture of ICT situation today. Special emphasis should be given to cyber-crime from big criminal organisations or even state-enabled actors. Thus the following aspects shall be addressed in the focus group workshop: cyber-attacks and cyber-crime, social network and privacy, information risks, data storage, vulnerability of existing and new information technologies (e.g. mobile phones).

5.3 ENVIRONMENT

The impact of environmental degradation and consequences of environmental changes are increasing associated with non-conventional nations of security (see findings of WP2, D.2.2). Considering the environment as a threat to individual, national or global security has created a new agenda in security studies. This has been mirrored in recent research programmes and projects, both at the European and national levels. Several of these projects now readily deal with environmental degradation, global warming and climate change. In addition, the interconnected problems of resource scarcity, epidemics and health-related risks, with the chronic impediments to economic growth and social stability that these trends could produce, are consistent features of several previous and existing projects.

An evolution with regard to the environmental dimension has been noted: (i) First, these types of concerns used to be the primary focus of non-governmental organisations. Now several organisations and institutions fund and do environmental security research, therefore propelling these themes into the main stream of security research. (ii) Second, more recent programmes tend to focus on the functional aspect of environmental security. Natural disasters in combination with man-made accidents, which are a combination of technological failures and environmental processes, are now key concerns of security research.

The following table details the result of the clustering and popularity by key dimensions from WP2:

Climate change and global warming
Natural or man-made major disasters and accidents
Major technological disaster (e.g. nuclear accident)
Oil spills
Droughts and heat-related hazards (above all in Southern Europe)
Alpine hazards, such as flash floods, avalanches and debris flows
Floods, alluviums, tropical storms and rain
Sea level rises
Landslides
Earthquakes

Strong winds
Freezes and cold fronts
Forest fires
Orbital debris
Near-earth (NEO) object collisions
Chronic diseases, epidemics and pandemics (e.g. HIV, malaria)
Resource scarcity (i.e. food, water, energy and minerals)
Environmental degradation
Biodiversity loss and invasive alien species
Water pollution
Land use and pollution
Air pollution
Waste management risks and dumping of hazardous waste (e.g. nuclear waste, CCS facilities)

Table 16 - Result of the clustering by key dimensions within environmental research from task 2.2

The findings of the desk research are the following:

Possible causes:

- Natural change of circumstances: drinking water (shortages due to climatic and geographical conditions, scarcity of anthropogenic influence, such as large construction projects), climate change (global warming, rising of sea levels), resource scarcity (food due to population growth, rare earths, energy such as oil and gas)
- By humans (insidiously) affected: increased emissions of greenhouse gases, chemical waste, long-term effects of genetic engineering, deforestation, soil erosion, diseases epidemics (pathogens in food or in the air), contaminants in fertilizers as well as detergents, monocultures

Possible aggressors:

- Population groups (war): struggle for living space, fight for water, food, raw materials
- Activists: notify us about deficiencies in research or policy
- Terrorists: ideology spread by contact or by other damage
- criminals (money): sales of vaccines (e.g. pig flu), cheap disposal biologically or chemically contaminated waste extortion
- Provided: accidents

Possible effects:

- Climate change: global warming, flooded land by rising sea levels, changes in ocean currents
- Conflict potential for conflict: water, food, energy resources, habitat
- Threat to humans: genetically modified foods, epidemics or diseases, natural disasters

The interviews of Task 4.1 demonstrated that we should focus on high system level hazards, which are able to trigger "classic" hazards (like flooding or heat waves), enhancing their probability of occurrence and amplifying their intensity or their effects. Apart from climate change important factors are seen in an efficient use of resources, loss of biodiversity or land grabbing. An important threat is also seen in environmental pollution. Both single incidents like chemical accidents as well as pollution due to non-point sources like the usage of fertilisers were mentioned by the interviewees (see chapter 3.2.3). Also the weak signal scanning showed the importance of pollution in general, population growth and invasive species (see chapter 4.2.3).

On the basis of those preparatory tasks we decided to set the focus in the workshop on environmental degradation. Following aspects were seen as important: biodiversity loss and invasive alien species, water pollution, land use and pollution, deforestation and soil erosion, population growth as well as potential conflicts related to the resource scarcity and resource distribution.

6 INPUT III: FOCUS GROUP WORKSHOPS

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

In general focus group research involves organised discussion with a selected group of individuals to gain information about their views and experiences of a topic. Focus group interviewing is particularly suited for interaction with experts and obtaining several perspectives about the same topic. One focus group for each field, cyber infrastructure, nuclear and environment will be conducted (see Figure 29).

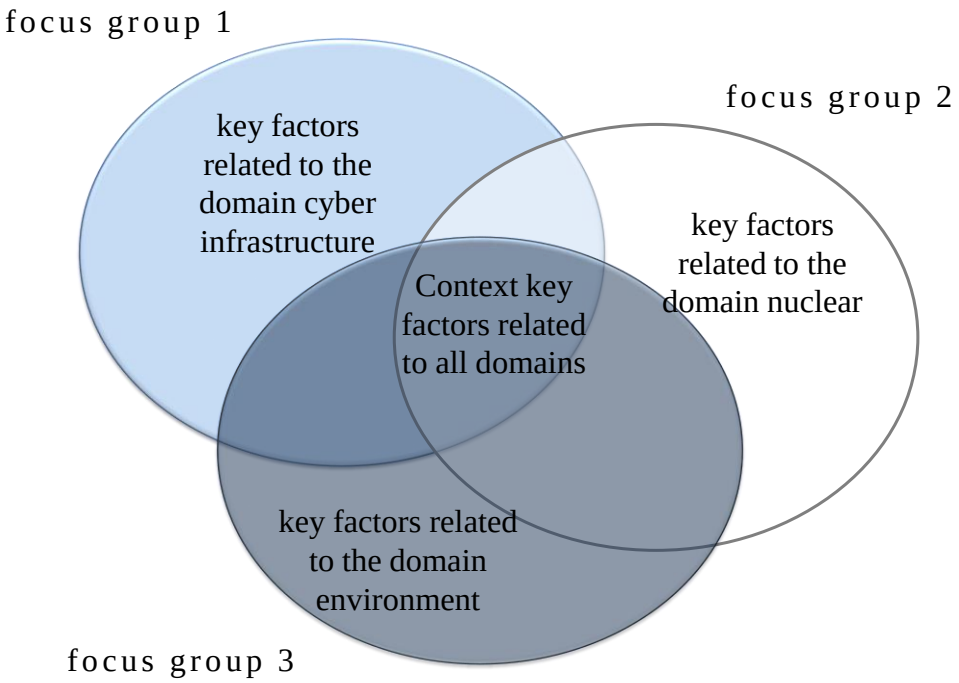


Figure 29 - Discussing the key factors on context and domain level in focus groups.

For this reasons we invited representatives of companies which deal with security in general, e.g. work in security businesses, develop or use security technologies as well as deal with further security aspects, like societal issues. For inviting persons, the desk research was used as well as the results from the interviews with key stakeholders. An overall environmental structure will serve as basis for a first workshop with the focus group.

6.1 STOCKTAKING OF THE KEY FACTORS

For preparing the focus group workshops, in particular the identification of the key factors, a wide range of sources was used, like various future studies and research works with focus on the future as well as the first input from the tasks 4.1 (Interviews with stakeholders) and 4.2 (IT-based weak signal mining) as outlined above. In the course of the reworking of the workshop results, these sources will be used also for the identification and description of uncertain developments of the key factors based on qualitative and quantitative data, also known as future projections.

Based on the desk research a wide range of future studies related to both context and the domains cyber infrastructure, nuclear and environment was collected. Additional the findings of task 2.2 were used, which provide an in-depth analysis of the key trends emerging from completed and on-going foresight and other relevant security projects, undertaken both in Europe and beyond.

We analysed almost 300 documents, which provide descriptions of different futures related to various aspects from the field of security in general as well as cyber, nuclear and environment. These future studies consider various time horizons. The following questions have been driven our inquiry:

- What are the key factors characterising and influencing the field of security today and in the future?
- What are the key factors characterising and influencing the domains cyber infrastructure, nuclear and environment?
- What kind of future projections describes the possible developments of the key factors?
- What are the present developments of the key factors?

The analysis relies largely on the systematic investigation of secondary sources. These documents represent different organisations, e.g. think tanks, other NGOs, research institutions and academia. Although we have particularly focused on European-funded research projects, we have also reviewed projects outside the EU. The identified factors clustered to several main groups build the base for the discussion in focus group workshops (see table 17-20 below).

6.1.1 Factors for the Context Scenarios

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

Table 17 - Factors for the context

6.1.2 Factors for Cyber Infrastructure

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

Table 18 - Factors for the domain cyber infrastructure

6.1.3 Nuclear Waste

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

Table 19 - Factors for the domain nuclear

6.1.4 Environment

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

Table 20 - Factors for the domain nuclear

7 OUTLOOK: APPROACH TO THE DEVELOPMENT OF CONTEXT AND THREAT SCENARIOS

For scenario development a 3-step process will be used (see Figure 30 below):

- Firstly, the draft context and threat scenarios will be developed.
- Secondly, the wild cards will be analysed to test the robustness of scenarios.
- Thirdly, scenarios will be validated by stakeholders.

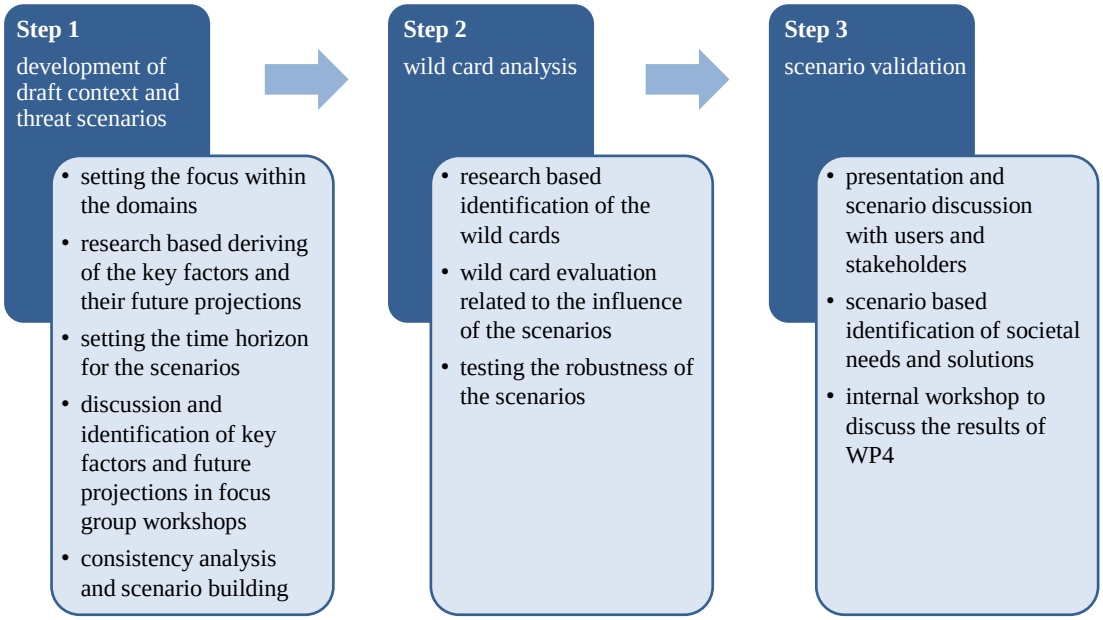


Figure 30 - 3-step-process for scenario development.

This document describes the first step of scenario development including the focus setting within the domains; the research based deriving of key factors and their future projections; setting the time horizon for the scenarios and preparation of the focus group workshops for identifying and discussing of key factors and future projections.

The results of the focus group workshops will be presented in the deliverable D.4.3. The consistency analysis and scenario building as well as the wild card analysis (step 2) and scenario validation (step 3) will be described in the deliverables D.4.4 and D.4.5.

8 ANNEX

8.1 INTERVIEW GUIDE

This annex only contains the interview guide for the interviews in the area of "nuclear material". The other interview guides for "cyber infrastructure" and "environmental issues" only differ in the question "*We are also interested in the development of the threats and hazards in the next 15 or 20 years. How do you think will the threats and hazards you have mentioned develop in this timespan?*" For "cyber infrastructure" we reduced the timespan to 5 years and for "environmental issues" we also asked for the development in a timespan of 15 to 20 years.

Task 4.1 Interviews with key stakeholders

Interview – Guide

"Current and future threats and societal needs"

Part 1 – Nuclear material

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

1 General Information

1.1 Interviewer

Organisation:

- ☐ Peace Research Institute Oslo (PRIO)
- ☐ Swedish Defence Research Agency (FOI)
- ☐ Hague Centre for Security Studies (HCSS)
- ☐ Trilateral Research & Consulting (TRI)
- ☐ Fraunhofer –Gesellschaft zur Förderung der angewandten Forschung eV (Fhg INT)
- ☐ Fraunhofer –Gesellschaft zur Förderung der angewandten Forschung eV (Fhg ISI)
- ☐ Austrian Institute of Technology (AIT)

Person:.....

1.2

1.3 Stakeholder:

Organisation:

.....

Person:

.....

Position:

.....

.....

.....

Category:

- ☐ Government
  - ☐ Policy makers
  - ☐ Regulators
  - ☐ Legislative
  - ☐ Administrative/ PM authority
- ☐ Industry
  - ☐ Large ☐ Medium ☐ Small
  - ☐ Manufacturers
  - ☐ System integrators
  - ☐ Suppliers/Distributors
  - ☐ Service Provider
- ☐ Academia/research institutions
- ☐ Think Tank
- ☐ Civil Society Organisation (CSO)
- ☐ The media
- ☐ The public

Focus:

- ☐ Law enforcement
- ☐ Environment
- ☐ Security/defence

☐ Social and economic development

☐ Civil protection

☐ Technology

☐ Health

☐ Critical infrastructures

Geography:

☐ EU

☐ National

Country: .....

☐ Transnational

1.4 Formalities

Date & time:

.....

Place:

.....

Modality:

☐ face-to-face ☐ by phone

The Expert got a copy of the ETTIS **data protection declaration**: ☐ Yes ☐ No

2 Interview:

2.1 Threats & Hazards

In our **definition** a threat results from intentional human activities and a hazard from unintentional acts, like accidents, systems failure or natural disasters.

To give you an example:

If we imagine for a moment that you are an expert in the area of "attacks from Mars". Then we would ask you now about the **threat** itself (hostile creatures, their weapon systems, their ability to fly, worst extent of damage, their resources, possible demands, ..) and about the **possible future development** of the threat (technical developments on Mars, know-how of Mars creatures, political & social developments on Mars, scarcity of energy and natural resources).

Which threats & hazards do you see in the area of nuclear material?

Possible choice of further questions:

- *We want to get a clear and complete picture of the threats and hazards in the area of nuclear material. What do we need to take into account?*
- *Is it possible to define organisations/groups who are responsible? – Which aims do they pursue?*
- *How vulnerable is our society regarding these threats & hazards and what areas/sectors are most vulnerable to these threats?*

We are also interested in the development of the threats and hazards in the next 15 or 20 years. How do you think will the threats and hazards you have mentioned develop in this timespan?

Possible choice of further questions:

- *Will there be new threats & hazards?*
- *Will the vulnerability of the society change and why?*

2.2 Societal Need

In our **definition** a societal need is some kind of requirement for response to a specific problem.

To return to the example of "Mars attacks":

A **societal need** in this case could consist of: protection of the people from Mars-attacks, protection of our infrastructure and our natural environment.

What do you see as the societal needs to result out of the before mentioned threats & hazards?

2.3 Solutions

(This part is "nice to have" in phase 1 and more important for phase 2 – after the focus group workshops.)

In our **definition** a security solution addresses one or more societal needs and is composed of capabilities. A **capability** consists of technical artifcats and/or institutional structures.

To return to the example of "Mars attacks":

We would like to talk about the **capabilities** needed (satellite early warning system, global crisis management system, stockpiling of specific drugs, ..), about **capabilities we might want in the future,** where research efforts are needed (new ways of interplanetary contact, technical solutions to overcome language problem) and possible **secondary effects** of the security solutions (financial issues, technical limits, ethical issues regarding satellite observation).

Which capabilities do we need to address these societal needs?

Possible choice of further questions:

- *Which technical systems do you suggest?*
- *Which institutional structures are needed?*

What capabilities do you think we should aim at in the future?

Possible choice of further questions:

- *In which research areas would you suggest to invest today?*

If we combine all these capabilities you mentioned to a security solution - do you see secondary effects of this security solution on the society?

Possible choice of further directions:

- *Financial limits*
- *Ethical & privacy issues*
- *Other risks*
-

8.2 INTRODUCTORY LETTER TO THE INTERVIEWEES

Dear Sir or Madam,

Herewith we would like to ask you if you would be so kind to support our EU project ETTIS by agreeing to do an interview with one of our project partners.

With this letter we would like to give you an overview of our project in general and the content of the interviews.

1. What is ETTIS?

European Security Trends and Threats In Society (ETTIS), is a EU FP7 collaborative research project focused on identifying and assessing opportunities for enhancing societal security, improving situation awareness and informing investment options for societal security. ETTIS aims to construct a comprehensive framework which can be used in the formulation of future decisions and security policies. The project, coordinated by the Peace Research Institute Oslo (PRIO) will run for 36 months from 1 January 2012 to 31 December 2014.

For further information please visit us at http://ettis-project.eu/.

2. Why do we need to conduct interviews?

One of the aims of our project is the development of future threat scenarios in three different domains (cyber infrastructure, nuclear material and environmental issues) as a basis for identifying societal needs.

To develop these scenarios we would like to conduct a series of interviews with experts, who will provide us with input regarding current and future threats and needs. We identified both security research end-users as well as representatives form civil society organizations. On the basis of these interviews we will identify the necessary key factors to fully describe the three domains for the development of the threat scenarios.

3. What topics will we address in the interview?

We will ask you about threats and needs in your area of expertise (in and around cyber infrastructure or nuclear materials or environmental issues).

We would ask you about the *threat itself*, about the *future development of the threat* and about the *societal needs*. We would also like to talk to you about possible *solutions or research proposals* and possible *secondary effects* of the *solutions*.

4. Who will be your interview partner?

The current work package is carried out by seven partners of the ETTIS consortium: (Peace Research Institute Oslo (PRIO), Swedish Defence Research Agency (FOI), Hague Centre for Security Studies (HCSS), Trilateral Research & Consulting (TRI), Fraunhofer-Gesellschaft (FhG) and Austrian Institute of Technology (AIT).

We would be most grateful if you could agree to be interviewed by us. The interview should take no longer than one hour.

If you have any further questions regarding the interview itself or the aims of ETTIS do not hesitate to contact us.

Dr. Sonja Grigoleit

Fraunhofer Institute for Technological Trend Analysis (INT)
Department Meta-Analyses and Planning Support
Appelsgarten 2, 53879 Euskirchen, Germany

Email: sonja.grigoleit@int.fraunhofer.de

Phone: +49-2251-18309

8.3 WEAK SIGNAL SCANNING

8.3.1 Annex 1: Google Trends results for "crisis"

Figure 31 - Quantity of searches, with the term "crisis".
Source: AIT, Google.

1.	Cuba	100
2.	Nigeria	83
3.	Zimbabwe	65
4.	Uganda	63
5.	Ecuador	56
6.	Nicaragua	52
7.	Fiji	52
8.	Chile	49
9.	Colombia	49
10.	Kenya	48

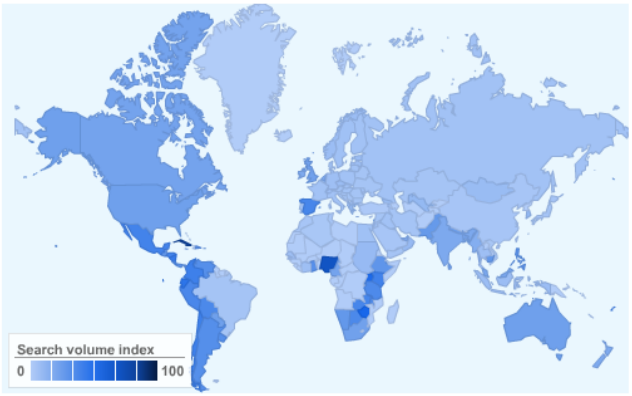


Figure 32 - Geographic distribution of searches for "crisis".
Source: AIT, Google.

Top searches			Rising searches	
1.	the crisis	100	crisis core	+3,300%
2.	la crisis	90	crisis loan	+600%
3.	financial crisis	50	global crisis	+350%
4.	crisis core	45	debt crisis	+250%
5.	economic crisis	30	final crisis	+250%
6.	crisis 2	30	final fantasy	+250%
7.	crisis what crisis	25	financial crisis	+250%
8.	final crisis	25	economic crisis	+150%
9.	crisis economica	25	economy crisis	+140%
10.	cuban missile crisis	25	crisis mundial	+130%

Figure 33 - Rising topics, similar to "crisis".
Source: AIT, Google.

8.3.2 Annex 2: Google Trends results for “disaster”

Figure 34 - Quantity of searches, with the term “disaster”.
Source: AIT, Google.

1.	Fiji	100
2.	Zimbabwe	77
3.	Kenya	70
4.	Uganda	60
5.	India	59
6.	Zambia	57
7.	Nepal	55
8.	Jamaica	55
9.	Trinidad and Tobago	54
10.	New Zealand	51

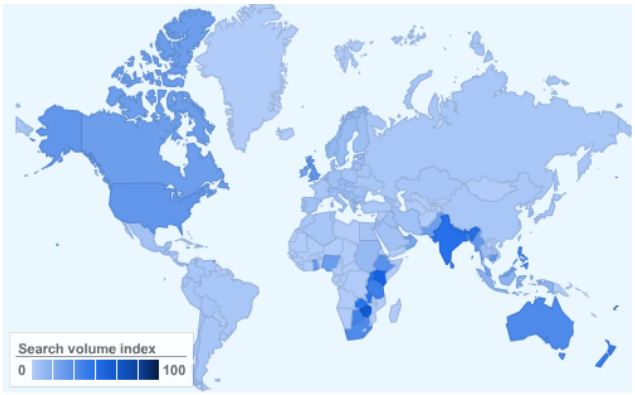


Figure 35 - Geographic distribution of searches for “disaster”.
Source: AIT, Google.

Top searches			Rising searches	
1.	disaster recovery	100	2012 disaster	Breakout
2.	disaster movie	90	walking disaster	+1,200%
3.	natural disaster	85	disaster movie	+800%
4.	disaster management	85	recipe for disaster	+800%
5.	disaster lyrics	65	japan disaster	+350%
6.	beautiful disaster	50	beautiful disaster	+150%
7.	disasters	35	beautiful disaster lyrics	+120%
8.	disaster plan	35	disaster lyrics	+70%
9.	disaster relief	35	disaster management	+70%
10.	chernobyl	30	disaster movies	+60%

Table 21 - Rising topics, similar to “disaster”.
Source: AIT, Google.

8.3.3 Annex 3: Google Trends results for “security”

1.	Lesotho	100
2.	Sierra Leone	88
3.	Timor-Leste	65
4.	Swaziland	64
5.	Botswana	62
6.	Uganda	56
7.	Rwanda	53
8.	United States	53
9.	Kenya	53
10.	Somalia	50

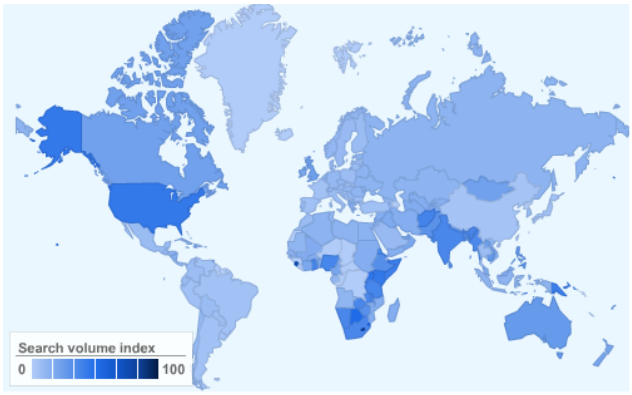


Figure 36 - Geographic distribution of searches for “security”.
Source: AIT, Google.

1.	United States	100
2.	Namibia	42
3.	Rwanda	32
4.	Philippines	31
5.	Tanzania	26
6.	Puerto Rico	25
7.	Uganda	19
8.	Jamaica	16
9.	Ghana	12
10.	Mauritius	8

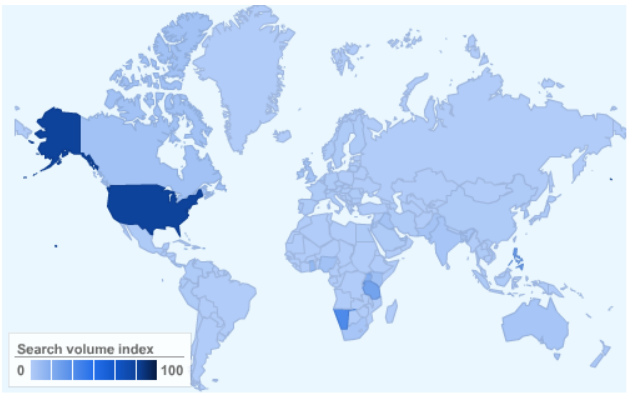


Figure 37 - Geographic distribution of searches for “social security”.
Source: AIT, Google.

1.	Belgium	100
2.	Netherlands	32
3.	United Kingdom	29
4.	Poland	24
5.	Germany	20
6.	Italy	14
7.	France	11
8.	United States	7

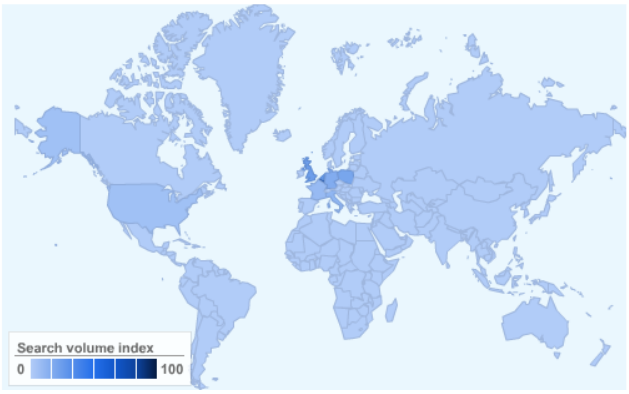


Figure 38 - Geographic distribution of searches for “European Security”.
Source: AIT, Google.

Top searches			Rising searches	
1.	european security strategy	100	1. esdp	Breakout
2.	european security policy	75	2. european security academy	Breakout
3.	european security defense	30	3. european security association	Breakout
4.	esdp	20	4. european security conference	Breakout
5.	european security studies	20	5. european security council	Breakout
6.	european security academy	15	6. european security journal	Breakout
7.	european security treaty	15	7. european security treaty	Breakout
8.	european security conference	15	8. european security policy	+80%
9.	european security research	15	9. european security strategy	+70%
10.	european security council	15	10. european security studies	+50%

Figure 39 - Rising topics, similar to "European Security". Source: AIT, Google.

8.3.4 Annex 5: Google Trends results for "nuclear threats"

1.	South Korea	100
2.	United States	31
3.	India	21
4.	Canada	18
5.	United Kingdom	10

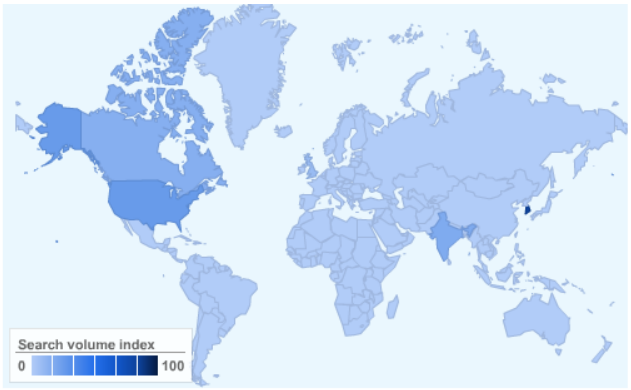


Figure 40 - Geographic distribution of searches for "nuclear security". Source: AIT, Google.

1.	United States	100
2.	India	95
3.	Cuba	90
4.	Myanmar [Burma]	86
5.	Philippines	81
6.	Pakistan	79
7.	Fiji	77
8.	Australia	76
9.	Mozambique	75
10.	Canada	72

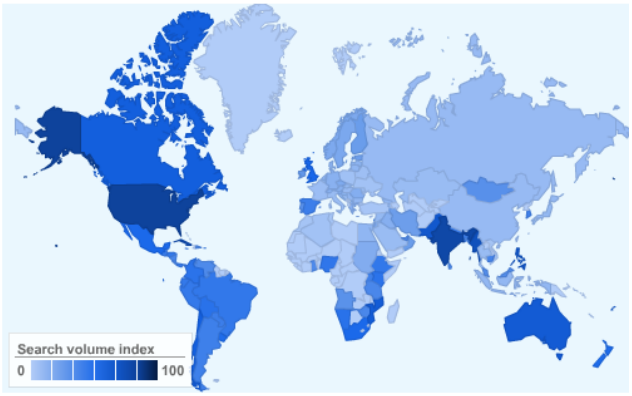


Figure 41 - Geographic distribution of searches for "nuclear". Source: AIT, Google.

8.3.5 Annex 6: Google Trends results for “environmental threats”

Top searches			Rising searches	
1.	pollution air	100	1. pollution essay	+250%
2.	water pollution	80	2. pollution facts	+100%
3.	the pollution	65	3. global warming	+90%
4.	pollution control	25	4. pollution in india	+90%
5.	environmental pollution	25	5. air pollution causes	+70%
6.	noise pollution	20	6. causes of pollution	+70%
7.	la pollution	20	7. china pollution	+70%
8.	noise	20	8. pollution control board	+70%
9.	what is pollution	20	9. pollution definition	+70%
10.	environment	20	10. types of pollution	+70%

Table 22 - Rising topics, similar to “pollution”.
Source: AIT, Google.

Figure 42 - Quantity of searches, with the term “water pollution”, from last 9 years .
Source: AIT, Google.

1.	Jamaica	100
2.	Trinidad and Tobago	88
3.	India	83
4.	Philippines	72
5.	South Africa	65
6.	Ethiopia	55
7.	Mauritius	53
8.	Nepal	53
9.	Lebanon	50
10.	Nigeria	49

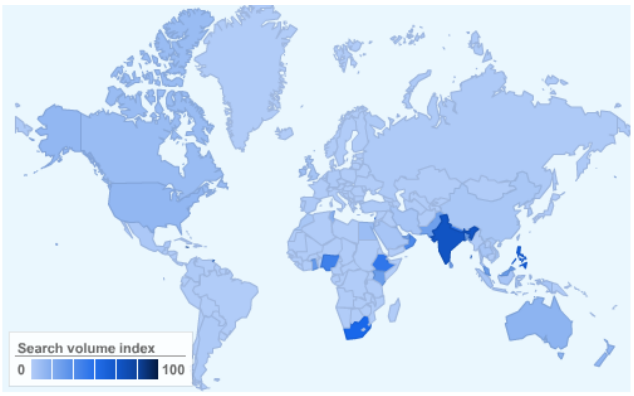


Figure 43 - Geographic distribution of searches for “water pollution”.
Source: AIT, Google.

Figure 44 - Quantity of searches, with the term "air pollution".
Source: AIT, Google.

1.	Philippines	100
2.	Trinidad and Tobago	96
3.	India	94
4.	Jamaica	92
5.	Mauritius	86
6.	Mongolia	83
7.	Nepal	82
8.	Ethiopia	82
9.	South Africa	69
10.	Cambodia	68

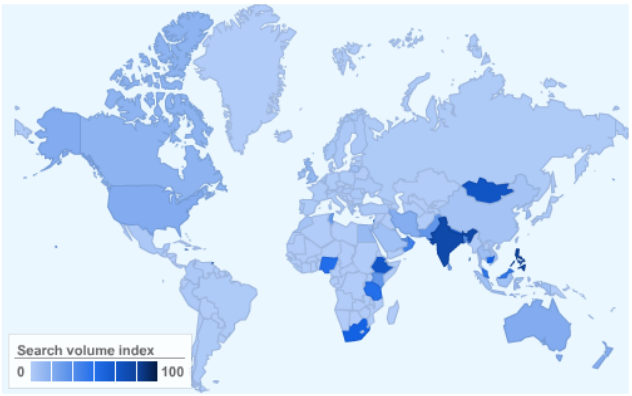


Figure 45 - Geographic distribution of searches for "air pollution".
Source: AIT, Google.

Figure 46 - Quantity of searches, with the term "light pollution".
Source: AIT, Google.

1.	Hong Kong	100
2.	United Kingdom	38
3.	United States	37
4.	Canada	34
5.	India	34
6.	Australia	19
7.	Germany	4

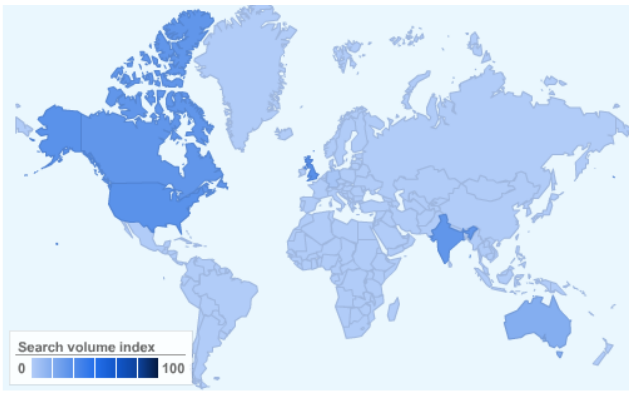


Figure 47 - Geographic distribution of searches for "light pollution".
Source: AIT, Google.

Figure 48 - Quantity of searches, with the term "noise pollution".
Source: AIT, Google.

1.	Trinidad and Tobago	100
2.	India	80
3.	Jamaica	70
4.	Philippines	48
5.	Pakistan	35
6.	Nigeria	31
7.	Singapore	23
8.	South Africa	23
9.	United Arab Emirates	20
10.	Ireland	17

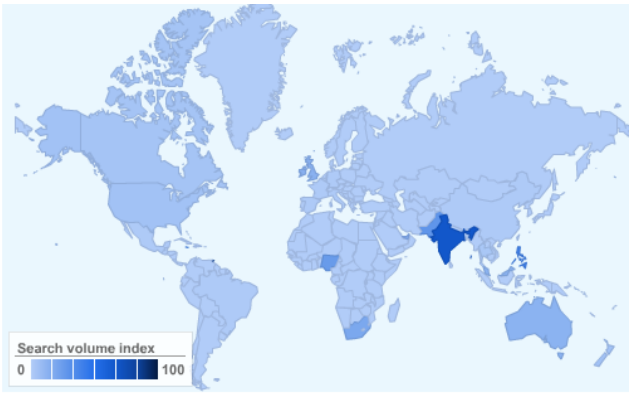
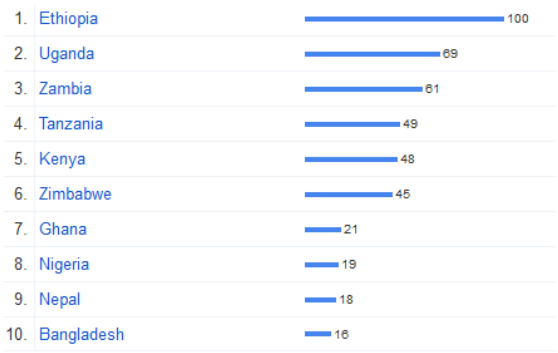


Figure 49 - Geographic distribution of searches for "noise pollution".
Source: AIT, Google.

Figure 50 - Quantity of searches, with the term "genetical engineering".
Source: AIT, Google.

Figure 51 - Quantity of searches, with the term "food security".
Source: AIT, Google.



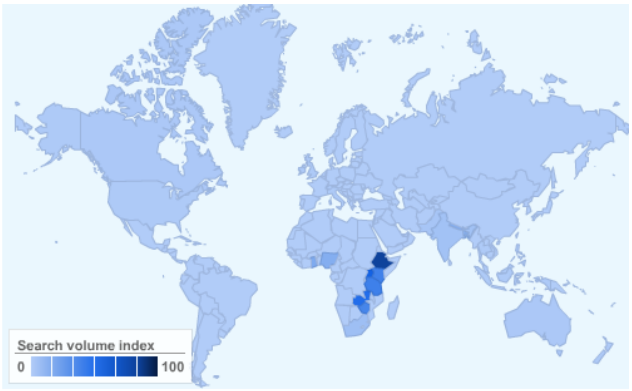


Figure 52 - Geographic distribution of searches for "food security".
Source: AIT, Google.

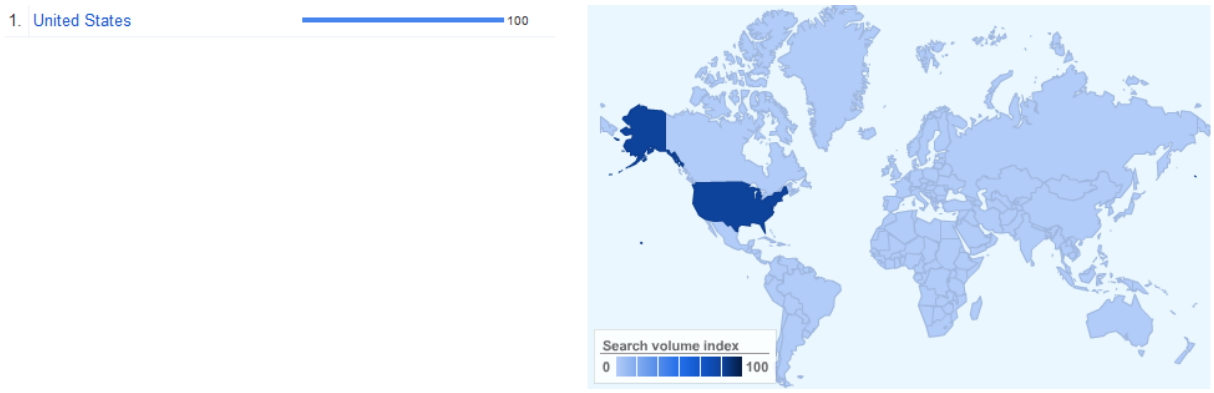


Figure 53 - Geographic distribution of searches for "environmental security". Source: AIT, Google.

Figure 54 - Quantity of searches, with the term "climate change". Source: AIT, Google.

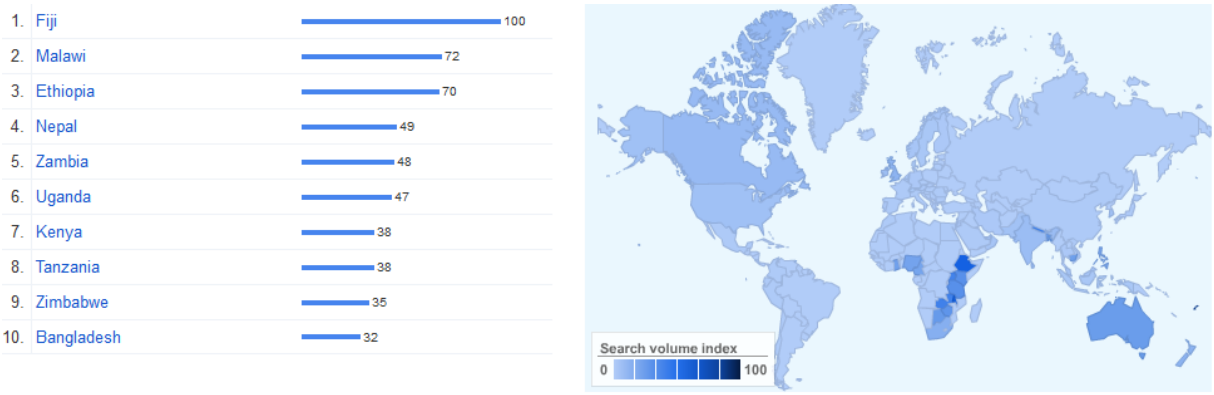


Figure 55 - Geographic distribution of searches for "climate change". Source: AIT, Google.

Top searches			Rising searches	
1.	global climate change	100	1. climate change 2007	Breakout
2.	global warming	60	2. copenhagen climate change	Breakout
3.	what is climate	30	3. climate change facts	+300%
4.	climate change effects	30	4. what is climate	+200%
5.	climate change conference	20	5. climate change adaptation	+190%
6.	climate change report	15	6. climate change definition	+100%
7.	climate change adaptation	15	7. climate change conference	+60%
8.	climate change impacts	15	8. climate change australia	+50%
9.	climate change causes	15	9. climate change causes	+40%
10.	climate change uk	15	10. climate change effects	+40%

Table 23 - Rising topics, similar to "climate change".
Source: AIT, Google.

Figure 56 - Quantity of searches, with the term "deforestation".
Source: AIT, Google.

1.	Ethiopia	100
2.	Jamaica	76
3.	Tanzania	73
4.	Trinidad and Tobago	63
5.	Mauritius	62
6.	Singapore	45
7.	Philippines	45
8.	Kenya	41
9.	India	41
10.	Nigeria	40

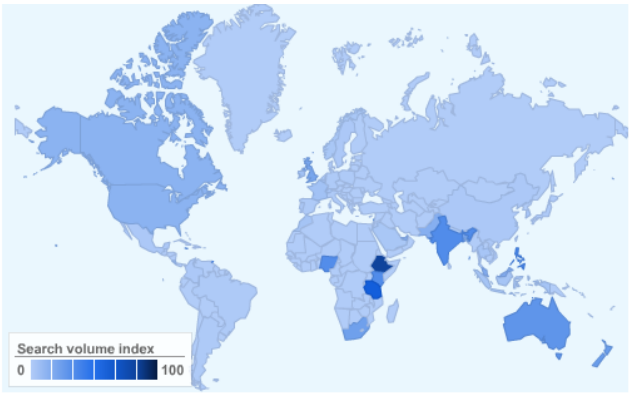


Figure 57 - Geographic distribution of searches for "deforestation".
Source: AIT, Google.

Top searches		Rising searches	
1. rainforest	100	1. deforestation definition	+170%
2. rainforest deforestation	100	2. deforestation facts	+160%
3. deforestation amazon	95	3. what is deforestation	+90%
4. deforestation effects	85	4. deforestation global warming	+70%
5. what is deforestation	80	5. about deforestation	+50%
6. global deforestation	75	6. deforestation causes	+50%
7. effects of deforestation	65	7. deforestation effect	+50%
8. deforestation causes	60	8. effect of deforestation	+50%
9. deforestation facts	55	9. causes of deforestation	+40%
10. deforestation global warming	55	10. global deforestation	+40%

Figure 58 - Rising topics, similar to "deforestation".
Source: AIT, Google.

Figure 59 - Quantity of searches, with the term "global warming".
Source: AIT, Google.

1.	Fiji	100
2.	Philippines	85
3.	India	80
4.	South Africa	70
5.	Trinidad and Tobago	62
6.	Nepal	59
7.	Mauritius	57
8.	Namibia	57
9.	Indonesia	53
10.	Botswana	52

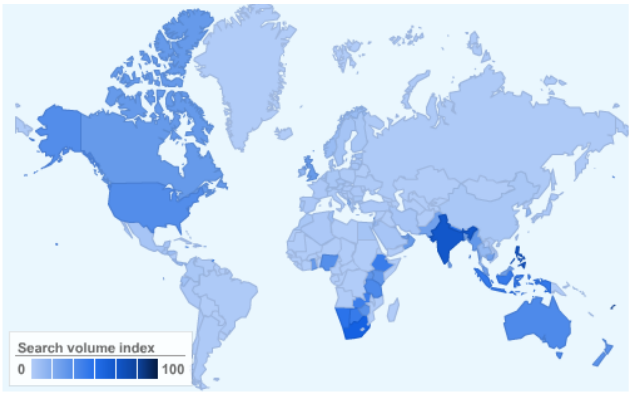


Figure 60 - Geographic distribution of searches for "global warming".
Source: AIT, Google.

Top searches			Rising searches	
1.	global warming\	100	1. global warming swindle	Breakout
2.	the global warming	15	2. global warming hoax	+850%
3.	global warming effects	5	3. al gore	+750%
4.	global warming causes	5	4. global warming essay	+300%
5.	global warming facts	5	5. global warming facts	+190%
6.	climate	5	6. stop global warming	+120%
7.	global warming effect	5	7. global warming kids	+90%
8.	about global warming	5	8. about global warming	+70%
9.	global climate change	5	9. global warming article	+70%
10.	climate change	5	10. global climate change	+60%

Table 24 - Rising topics, similar to "global warming".
Source: AIT, Google.

Figure 61 - Quantity of searches, with the term "pollution".
Source: AIT, Google.

1.	Fiji	100
2.	Benin	93
3.	India	83
4.	Trinidad and Tobago	71
5.	Mauritius	65
6.	Lebanon	64
7.	Jamaica	64
8.	Nigeria	53
9.	Tunisia	53
10.	Philippines	51

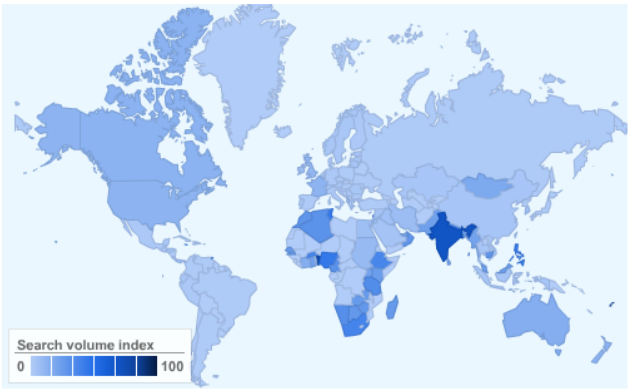


Figure 62 - Geographic distribution of searches for "pollution".
Source: AIT, Google.

Figure 63 - Quantity of searches, with the term "plastic trash".
Source: AIT, Google.

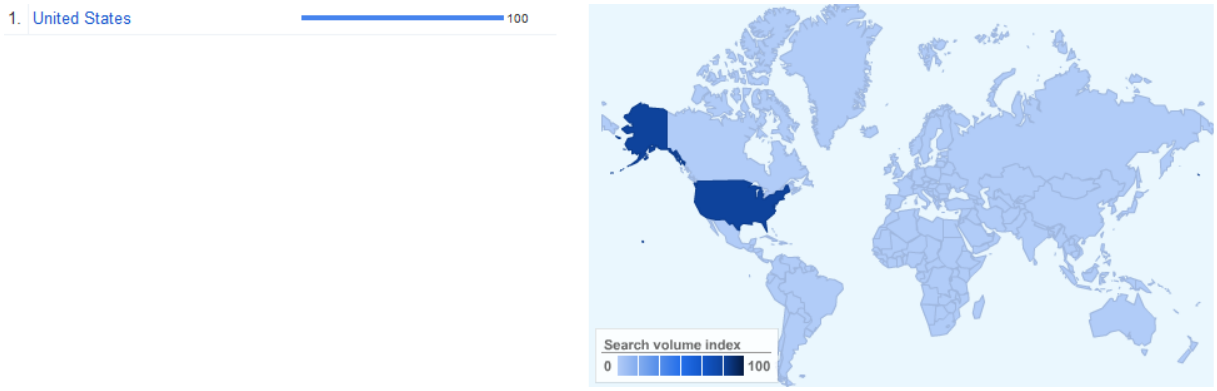


Figure 64 - Geographic distribution of searches for "plastic trash".
Source: AIT, Google.

Figure 65 - Quantity of searches, with the term "Loss of Biodiversity".
Source: AIT, Google.

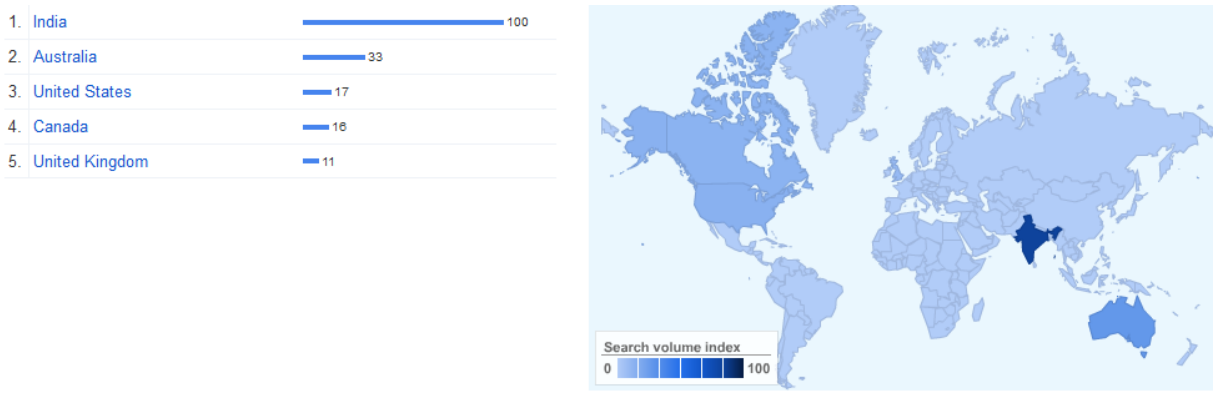


Figure 66 - Geographic distribution of searches for "Loss of Biodiversity".
Source: AIT, Google.

Figure 67 - Quantity of searches, with the term "Rising Sea Levels".
Source: AIT, Google.

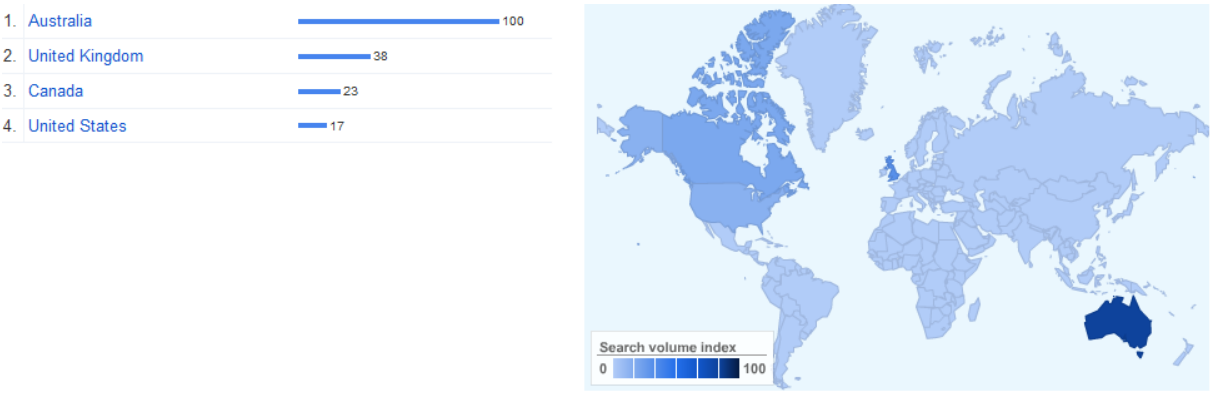


Figure 68 - Geographic distribution of searches for "Rising Sea Levels".
Source: AIT, Google.

Figure 69 - Quantity of searches, with the term "Population Growth".
Source: AIT, Google.

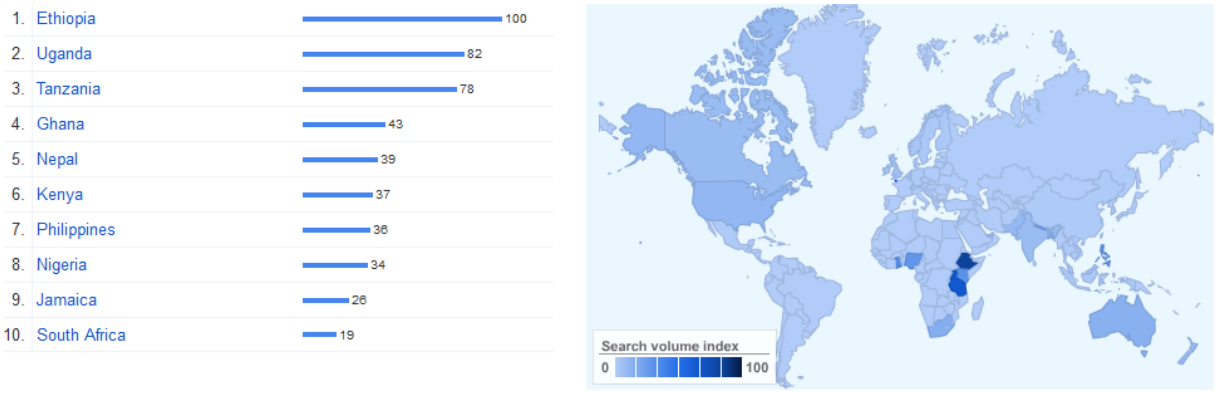


Figure 70 - Geographic distribution of searches for "Population Growth".
Source: AIT, Google.

Figure 71 - Quantity of searches, with the term "invasive species".
Source: AIT, Google.

1.	United States	100
2.	Canada	84
3.	South Africa	36
4.	Ireland	29
5.	Australia	27
6.	New Zealand	27
7.	United Kingdom	15
8.	India	7
9.	Germany	2

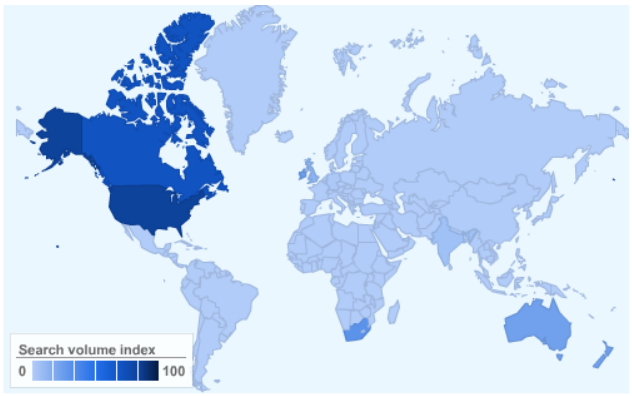


Figure 72 - Geographic distribution of searches for "invasive species". Source: AIT, Google.