



Funded by the European Commission

Seventh Framework Programme



CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D 2.1 Roadmapping methodologies and guidelines for information collection and assessment

Date of deliverable: 31/08/2014

Actual submission date: 12/09/2014

Start date of the Project: 1st June 2014. Duration: 24 months

Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab

Version: 1.5

**Project funded by the European Commission Directorate-General Home Affairs
in the Prevention of and Fight against Crime Programme**

Restriction Level

PU	Public	✓
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission)	



Roadmapping methodologies and guidelines for information collection and assessment

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 65

Revision history

Version	Object	Date	Author(s)
0.1	Creation	26/06/2014	SUPSI
1.0	Revision	21/07/2014	SUPSI, UNICA
1.1	Revision	31/07/2014	All task partners
1.2	Updated section 5.2 on ontology, and added ethical and legal aspects	02/09/2014	SUPSI
1.3	Addressed partners' contributions	03/09/2014	SUPSI, UNICA
1.4	Addressed partners' contributions, added list of acronyms and section 5.5 "Form to present the results"	11/09/2014	SUPSI
1.5	Addressed partners' contributions	12/09/2014	SUPSI, UNICA
1.6	Final draft	12/09/2014	SUPSI, UNICA





D2.1

Guidelines for information collection and assessment

Responsible

Angelo Consoli, Fabio Schiavoni (SUPSI)

Contributor(s)

Luca Didaci, Giorgio Fumera, Giorgio Giacinto, Fabio Roli, Davide Ariu (UNICA)

Javier Martinez Torres, Jorge Lopez Hernandez-Ardieta (INDRA)

Olga Segou (NCSRD)

Erik Tews (TUD)

Lorenzo Cavallaro (RHUL)

Jart Armin (CDF)

Clement Guitton (MELANI)

Summary:

The deliverable document D2.1 is the first, in chronological order, of the CyberRoad project. It has therefore four basic purposes: proposing a definition and characterization of the problem space; presenting a survey on the available methodologies suitable to define a roadmap to conduct cyber security researches; defining an ontology which covers the cyber crime / cyber security domain space; designing guidelines for collect and assess information from potential stakeholders of cyber security-related technologies.

Keywords: *attack, cyber crime, cyber security, cyberspace, domain space, metric, ontology, problem space, research gap, roadmap, vulnerability, cyber ethics*



1 TABLE OF CONTENTS

1	Table of contents	5
2	Introduction.....	9
3	Cyber Security: definitions and the problem space	11
3.1	<i>CYBER CRIME</i>	11
3.2	<i>CYBER TERRORISM</i>	11
3.3	<i>CYBER SECURITY</i>	11
4	Roadmapping Methodologies.....	13
4.1	<i>INTRODUCTION</i>	13
4.2	<i>A SURVEY OF PREVIOUS WORK ON SCIENCE AND TECHNOLOGY ROADMAPPING</i>	13
4.2.1	<i>Roadmap categories: normative and exploratory</i>	14
4.2.2	<i>Roadmap creation</i>	15
4.2.3	<i>Examples of roadmapping process</i>	17
4.2.4	<i>Data sources, and information collection and processing</i>	24
4.2.5	<i>Roadmap representation and visualization</i>	25
4.2.6	<i>Evaluation of roadmap quality</i>	29
4.2.7	<i>Example of a roadmap of interest to the CyberRoad project: eGovRTD2020</i>	31
4.3	<i>FIVE KEY ISSUES FOR SCIENCE AND TECHNOLOGY ROADMAPPING</i>	36
4.4	<i>A FIRST PROPOSAL FOR THE CYBERROAD ROADMAPPING METHODOLOGY</i>	37
4.4.1	<i>The context of the CyberROAD project and the need for a roadmapping methodology</i>	38
4.4.2	<i>A proposal for the CyberRoad roadmapping methodology</i>	39
5	Guidelines for Information Collection and assessment	46
5.1	<i>CYBER SECURITY PANORAMA</i>	46
5.1.1	<i>The drivers and actors of cyber crime</i>	46
5.1.2	<i>Reasons behind cyber security</i>	47
5.2	<i>CYBER SECURITY ONTOLOGY</i>	47
5.2.1	<i>What is an Ontology?</i>	48
	<i>A method to define ontologies</i>	48
5.2.2	48
5.2.3	<i>List of all possible assets and aspects related to cyber crime</i>	49
5.2.4	<i>Collection of all Cyber security aspects</i>	52
5.2.5	<i>Stakeholders of Cyber security</i>	54
5.2.6	<i>Classification of the targets</i>	54
5.2.7	<i>Description of the Ontology</i>	54
5.2.8	<i>An Ontology for cyber security</i>	54



5.2.9	<i>Standard languages for the Ontology</i>	58
5.3	<i>DATA COLLECTION METHODOLOGY</i>	58
5.3.1	<i>Sources of information and related classification</i>	59
5.3.2	<i>Methodology to define groups of people to be interviewed</i>	59
5.3.3	<i>Methodology of interviewing</i>	60
5.3.4	<i>Metrics for ranking of the sources</i>	60
5.3.5	<i>Template of the questionnaires</i>	61
5.4	<i>GUIDELINES TO ASSESS AND REPORT INFORMATION</i>	61
5.5	<i>FORM TO PRESENT THE RESULTS</i>	62
6	<i>Conclusions</i>	62
7	<i>References and bibliography</i>	62

List of Tables

Table 1:	Actors of cyber crime / cyber terrorism	47
Table 2:	Level of expertise of interviewees	59
Table 3:	Interviewing methodologies	60
Table 4:	Ranking of sources	60

List of Figures

Figure 1:	Data flow of the procedure to reach D2.1 outcomes	10
Figure 2:	An exploratory-goal-oriented roadmap taxonomy (Beeton, 2007).....	15
Figure 3:	Overview of the policy-oriented roadmapping process proposed in [IEA 2010].....	17
Figure 4:	Template of the graphical representation of the roadmap in [Kerr 2013].	18
Figure 5:	The graphical representation of the roadmap in [Kerr 2013].....	20
Figure 6:	Sketch of the roadmapping process described in [Kerr 2013], with reference to the roadmap shown in Figure 3.....	21
Figure 7:	Input factors for scenario-based technology forecast [Geschka 2013].	22
Figure 8:	The process of scenario-based, exploratory roadmapping of [Geschka 2013].	22

Figure 9: Example of a scenario-based, exploratory TRM [Geschka 2013], for a fuel cell application on a micro level.	24
Figure 10: The roadmap template of [Beeton 2013].	27
Figure 11: High-level view of the roadmap representation of [Beeton 2013].....	28
Figure 12. An example of the information presented in the graphical representations of the detailed insights, for one of the key points of Figure 10.....	28
Figure 13: Overview of the eGovRTD2020 roadmapping approach.	32
Figure 14: Methodology for scenario building in eGovRTD2020.	33
Figure 15: Characterization of scenarios in eGovRTD2020.....	33
Figure 16: The gap analysis methodology adopted in eGovRTD2020.....	34
Figure 17: Overview of the eGovRTD2020 operational methodology.....	35
Figure 18: Left: a template for the description of the research actions, means of actions, key actors and time-frame of action, related to a given research theme identified in eGovRTD2020 (in this example: "Trust in eGovernment"). Right: a template of the roadmap chart indicating the actions in a time-scale, for the same research theme on the left.....	36
Figure 19: The CyberROAD Evidence-Based Practice Triad.....	42

Acronyms and abbreviations

DoW	Description of Work
WP	Work Package

The deliverable D2.1 is the first, in chronological order, of the CyberRoad project and it has two main purposes: the first purpose is to present a survey on the available methodologies suitable to define a roadmap to conduct cyber security researches;; the second purpose is to design guidelines for collect and assess information from potential stakeholders of cyber security-related technologies. The information collected represents a base for further in-depth discussion during the course of the project, and further will be used to define the methodology for risk assessment ranking (T2.2)

The deliverable D2.1 is composed of the following sections:

Section 2 – Cyber Security: Definitions and the Problem Space

In this section the definition of cyber crime and cyber security are given, along with a presentation of the main concepts in the cyber security problem space.

Section 3 – Roadmapping methodologies

In this section an overview of the literature on Science and Technology roadmapping is given. Proposed methodologies, best practices, guidelines and case studies are summarized. On the basis of this review, the key methodological issues that have to be addressed in WP2 are identified, and a first proposal of the CyberRoad roadmapping methodology is proposed.

Section 4 – Guidelines for Information Collection and Assessment

Section 4 has as its main objective the definition of a template for the questionnaires that will be used to gather information from stakeholders and the production of guidelines to assess and report information. The following data flow diagram schematizes the procedure adopted to reach the goals envisaged by T2.1.



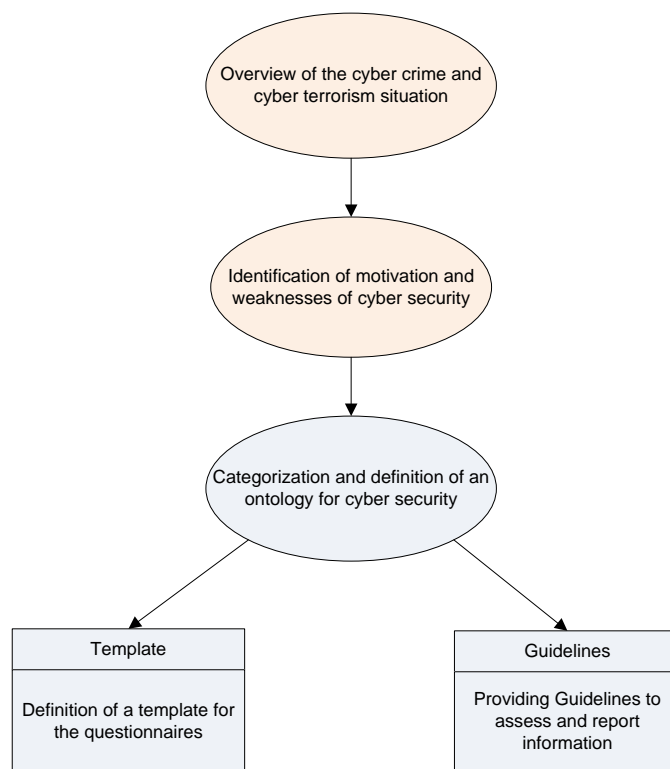


Figure 1: Data flow of the procedure to reach D2.1 outcomes

Section 4 starts presenting an overview of the current cyber security panorama, in terms of actors and drivers of cyber crime / cyber terrorism, and the motivations behind them. The actual and potential targets of the attacks are identified and the reason for cyber security is deduced. Eventually, the current situation of cyber security facilities is analyzed and potential vulnerabilities are identified (section 5.1 – Cyber security panorama).

It then defines a common-base cyber security taxonomy (ontology). In order to reach this objective, the actual and potential cyber crime / cyber terrorism threats, attackers, targets, motivations and technological means are categorized. In particular, current and potential categories of stakeholders of cyber security are inferred. Finally, the ontology is presented (section 5.2 – Cyber security ontology).

Having circumscribed the cyber security problem space, a template for the questionnaires that will be used to collect information from the identified stakeholders is defined. Moreover, a metric for the ranking of information sources is defined and used in the template (section 5.3 – Data collection methodology).

According to the contents of the questionnaires template defined in the previous subsection, guidelines to conduct information gathering and to assess and report the collected data are produced (section 5.4 – Design of guidelines to assess and report information).

3.1 CYBER CRIME

Definition of cyber crime

Cyber crime encompasses two forms of criminal activities: the use of computer system to enable traditional form of criminal activity (e.g., child pornography, money laundering); and the use of a computer system to launch a cyber attack (as understood by the aforementioned definition).

Cyber crime by definition is any harmful act committed from or against a computer or network, it differs according to McConnell International, “from most terrestrial crimes in four ways: they are easy to learn how to commit, they require few resources relative to the potential damages caused, they can be committed in a jurisdiction without being physically present in it and fourthly, they are often not clearly illegal. Another definition given by the Director of Computer Crime Research Centre (CCRC) during an interview on the 27th April, 2004, is that “cyber crime (‘computer crime’) is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. In essence, cyber crime is crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbol or any other way and transferred through local and global networks. [ICSJWG 2011].

Cybercrimes can be basically divided into 3 major categories [ICSJWG 2011]:

1. Cyber crimes against people.
2. Cyber crimes against property.
3. Cyber crimes against government (public).

3.2 CYBER TERRORISM

Definition of cyber terrorism

The use of a cyber attack breaching components of information security, instigated in order to achieve political motives largely of a subversive nature, and resulting in either physical destruction or loss of life.

3.3 CYBER SECURITY

Definition of cyber security

The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.

Information security refers to measures taken to protect or preserve information on a network as well as the network itself. The alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe has demanded that significant attention be paid to critical information infrastructure protection initiatives. [CSEC 2013]

Cyber Security refers to that part of Information security focused on the Cyberspace(in particular, on the Internet).

THE ABOVE DEFINITIONS WILL BE REVISED FURTHER ALONG THE NEXT TASKS AND DELIVERABLES OF THE PROJECT.

4.1 INTRODUCTION

According to the DoW of the CyberRoad project, the goal of WP2 is *to supervise and coordinate the work of all the other WPs in order to create the research roadmap*, that is the main product of the project. It is easy to see that this goal of WP2 demands to specify a *methodology* for the creation of the CyberRoad roadmap. The definition of a methodology for the creation of a roadmap is a problem that has been addressed by previous work in many fields (technology, economics, engineering, etc.; see the next section) and is usually referred to as “**science and technology roadmapping**”.

The aim of this section is to identify the tasks and issues that have to be addressed in WP2 in order to define the **CyberRoad roadmapping methodology**. This methodology will be the main tool for the coordination tasks of WP2 and, therefore, it will be used to coordinate and supervise the activities of all the other WPs. To this end, an overview of previous work on science and technology roadmapping is given first, with a focus on roadmaps for policymakers, which is the most relevant case for the CyberRoad project. Proposed methodologies, best practices, guidelines and case studies are examined. Then, based on such a literature overview, we identify **5 key issues** related to the roadmapping methodologies that have to be addressed by WP2. Finally, we briefly discuss the key aspects of the CyberRoad roadmapping methodology, which will be explored in full within Task 2.2 (“Methodology for Risk Assessment Ranking”) and reported in the upcoming D2.2 deliverable (titled “Risk Assessment Ranking methodology”). The work presented herein will establish a concrete basis for the all WP2 actions towards the definition of the **CyberRoad roadmapping methodology and the production of the final CyberRoad Research Roadmap**.

4.2 A SURVEY OF PREVIOUS WORK ON SCIENCE AND TECHNOLOGY ROADMAPPING

Technology Roadmaps (TRMs), or Science and Technology roadmaps (S&TRM), are currently widely used at business and policy levels to support technology strategy development and implementation [Londo 2013]. S&TRM have been adopted since mid-1980s by corporations and industries for strategic planning of S&T resources. Corporate- and industry-level S&TRMs usually focus on a single product, product family, or technological sector, and have well defined goals related to supporting the development of new products or technologies: *given a predefined, desirable state of the future, the roadmap defines how to attain it from the current state*. Since the mid-1990s, the S&TRM methodology has been increasingly exploited also by research institutes and think-tanks for providing intelligence to policymakers, with the aim of optimizing public R&D investments and ensuring their relevance to society, also in fields different from R&D like defence and economy [Da Costa 2005]. With respect to corporate- and industry-level S&TRMs, policy-oriented ones are often characterized by wider and less well defined scope and goals (like far reaching societal challenges), and usually involve social, cultural, political, legal and economical dimensions, besides the technological one. Schematically, company- and industry-level TRM/S&TRM are for experts, whereas policy-oriented ones are for generalists [Da Costa 2005]. The role of S&TRM for policy intelligence is pointed out in [Da Costa 2005]: *“It can be an important input in the selection of research priorities by highlighting the emerging S&T themes likely to impact on policy in the coming years. In a recent benchmarking study, roadmapping was highlighted as one of the ‘recommended best practices’ for the selection of priorities in R&D programmes since it does not only identify the bottlenecks that need to be addressed within a realistic time frame, but it can lead to a high degree of consensus when the potential beneficiaries are involved in the agenda-setting process”*. This kind of S&TRM is considered in [Jeffrey 2013] as still emerging, and its main goal is identified as political persuasion: *“These roadmaps are written by multiple organisations, often at the sector level, to persuade governments that they should*



implement the actions and recommendations set out."

In this section, a short review of scientific papers and case studies dealing with S&TRM is given, with a focus on roadmapping for policy intelligence. The goals and scope of this review are narrowed to the goals of the CyberRoad project. Namely, we focused on the issues that have been considered the most important for the definition of the roadmapping methodology of the project.

We first describe a basic categorization of roadmapping approaches into *normative* and *exploratory*, discuss some methodological approaches proposed for policy-oriented S&TRMs, and provide two examples of normative and exploratory roadmap construction. We then focus on three specific issues for which extensive guidelines and good practices are available: how to select data sources, and collect and process information; how to construct graphical representation of roadmaps; and how to ensure and evaluate their quality. We finally describe an example of a roadmap that we consider of interest for the CyberRoad project.

4.2.1 ROADMAP CATEGORIES: NORMATIVE AND EXPLORATORY

The main approaches underlying S&TRM applications can be broadly categorized into *goal-oriented* (or *normative*), and *exploratory*, depending on the approach used for envisaging the future:

- In *goal-oriented*, or *normative* roadmaps, a single desirable state of the future is envisaged, and roadmapping consists of *finding the paths leading from the present to this state* [Da Costa 2005]. This kind of roadmap outlines a sequence of activities and actions to define how a predefined strategy may be implemented, or a predefined objective achieved [Beeton 2007, 2008, 2013]. In the words of [Londo 2013], normative TRMs build a desired future state and describe actions and milestones required to reach it. This implies a relatively short time horizon (6 months up to 5 years, depending on the application field), and the main quality of the roadmapping output is to be "scientifically accurate" [Da Costa 2005]. Typically, in a normative roadmap the goals are provided in detail by high-level decision makers or final end users (e.g., by policymakers) [Kerr 2013]. This approach is commonly used in corporate and industry TRMs [Da Costa 2005]. It has also been recently proposed to support planning the implementation of government's policies for public services (e.g., defence, energy, health, transport): such policies are often outlined in white/command papers embodying a country's future vision, and their realization is the task of specific government departments/agencies through strategic planning activities [Kerr 2013].
- The *exploratory* approach is commonly used in scenario building, and has been introduced in S&TRM in the 2000s [Da Costa 2005]. It starts from the postulate that the future cannot be predicted and that various alternative futures of a single present state should be considered, including rupture scenarios and major technological breakthroughs [Da Costa 2005]. One of the goals of exploratory roadmaps is to enhance future outlook or foresight, allowing one to better understanding an industrial, technological or social landscape, or a competitive position, and to subsequently define clear and specific objectives [Beeton 2013]. The investigation of non-technical fields of influence can play a major role in scenario-based S&TRMs [Geschka 2013], since the development of a technology is also influenced by market-related, societal and economic factors. In particular, scenario-based TRMs are mainly an instrument of technological forecasting, but are not yet a planning instrument [Geschka 2013]. Exploratory S&TRMs can be used to inform the policy agenda by highlighting the emerging S&T themes that are likely to impact policy changes in the coming years, or as an exploration tool to anticipate long term needs which are not necessarily yet articulated, as well as emerging, trans-disciplinary or peripheral issues which have not yet received wide attention [Da Costa 2005]. In the exploratory approach the time horizon can be much longer than in the normative one. For example, in the case of slow-moving sectors (e.g. energy), exploratory roadmaps may even extend to decades. Moreover, the roadmap could take into



account hypothetical or visionary developments [Da Costa 2005], which is a particularly interesting feature when exploring fast-changing industries (such as Cyber-Security).

Normative and explorative roadmaps can thus be very different, having different starting points and goals. It is worth to note that an exploratory-goal-oriented roadmap taxonomy is proposed in [Beeton 2007, 2013], as shown in Figure 2, which suggests that "hybrid" roadmaps with both normative and explorative elements can also exist. Such hybrid roadmaps could be of interest for the CyberRoad project, given the particular features of cyber crime and cyber terrorism that could be difficult to capture in a single roadmap (normative or exploratory).

An example of policy-level, normative S&TRM is the "Healthcare Technologies Roadmap: Effective Delivery of Healthcare in the Context of an Ageing Society", mentioned in [Da Costa 2005], developed in the context of a pilot project related to major socio-economic challenges facing Europe. Another example is the case study TRM based on the Australian Government's Defence White Paper and the Royal Australian Navy's [Kerr 2013] (see Figure 5), which is described in more detail below.

Examples of policy-level, exploratory roadmaps are the "Ambient Intelligence in Everyday Life" roadmap, developed in the context of the same pilot project mentioned above [Da Costa 2005], and the roadmap produced by the EU FP6 project "Roadmapping eGovernment Research - Visions and Measures towards Innovative Governments in 2020" [Codagnone 2007] (see, e.g., Figure 18). The latter is also described in detail below.

The choice between the normative and the exploratory approach depends on the S&TRM context. [Da Costa 2005] points out that an important issue in the preparatory phase of a policy intelligence S&TRM is to assess the sensitivity and the needs of the roadmap targets in this respect; in particular, the trade-off between the "scientific validity" (which can be attained to a greater extent in normative roadmaps) and the "vision" of the future (which is more easily addressed by exploratory roadmaps) in the roadmapping output should be taken into account.

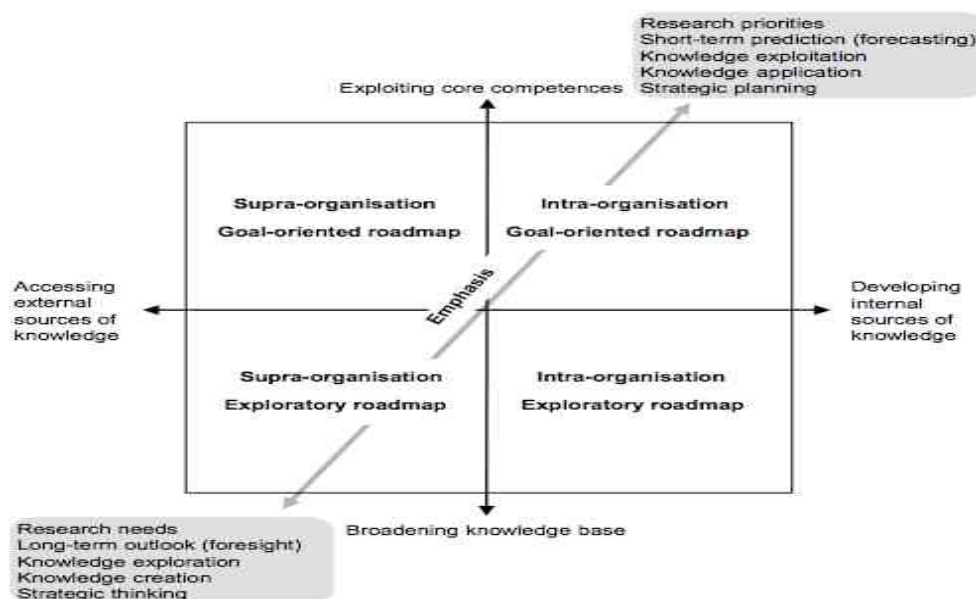


Figure 2: An exploratory-goal-oriented roadmap taxonomy (Beeton, 2007)

4.2.2 ROADMAP CREATION

Although S&T roadmapping has been the subject of some methodological studies so far [Lizaso 2004;

Möhrle 2013], it has not yet reached maturity as a discipline on its own [Codagnone 2007; Carvalho 2013]. No single definition of TRM/S&TRM exists either, due to their widespread usage, as well as no single paradigm or standard for roadmap construction. Several methodologies, guidelines and procedures have nevertheless been proposed so far for roadmap construction [Da Costa 2005; Industry Canada; Londo 2013]. Some of them are available in the form of case studies [Kerr, 2013], or as the results of previous S&TRM projects [Codagnone 2007]. Here we focus on two works that addressed this issue in detail in the context of policy-oriented S&TRMs [Da Costa 2005; Londo 2013], and illustrate some remarkable general points. We then give two examples of normative and exploratory roadmap construction.

In [Da Costa 2005] a pilot roadmapping project specifically targeted to policy intelligence in the EU context was described. It resulted in two roadmaps on "Ambient Intelligence in Everyday Life", and on "The Healthcare Technologies Roadmap: Effective Delivery of Healthcare in the Context of an Ageing Society". In this project, a roadmap construction methodology made up of three main steps was developed: 1) preparatory phase, 2) implementation phase, 3) validation and evaluation. Detailed guidelines are provided for each step. We summarize here the issues that have to be addressed in the preparatory and implementation phase, according to [Da Costa 2005] (a discussion on each of them can be found in [Da Costa 2005]). The issues related to the validation/evaluation phase are discussed in more detail later in this section.

During the **preparatory phase**, the following issues should be addressed: guaranteeing the necessary commitment of the roadmap clients/targets; composition of the core team; involvement of external participants; time and resources for meetings; exploiting in-house and external knowledge and expertise; assessment of the needs (a crucial issue in S&TRM for policymakers, where the goals are likely to be less clearly defined than in corporate/industry roadmapping); precise definition of the focus and scope; definition of the trade-off between the roadmap scope and breadth, and the depth of the analysis; approach to the "future" (either normative or exploratory); identifying the information sources and defining how to collect and process it.

The **implementation phase** leads to the construction of the roadmap, and consists of collecting, synthesising and validating the information, and representing the trends within graphic displays associated with support documents. It has been pointed out that *"aiming at building a single, standardized and general methodology [for roadmap creation] is neither practical nor desirable"*, and that *"the approach should be based on a light and modular process using a 'methodological toolbox' with different modules depending on the roadmapping areas, issues, context and objectives."* Some key factors for a successful roadmap, to be taken into account during the implementation phase, are also pointed out.

In [Londo 2013] about 200 existing TRMs related to climate change adaptation and mitigation technologies are analysed, including TRMs targeted to policymakers. The diversity in the underlying methodologies is pointed out. In particular, [IEA 2010] is mentioned as a relevant example of roadmap construction process in the policymaking context, and as an excellent standard for best practices in TRM construction. In [IEA 2010] a general roadmapping process is described, which focuses on the need for common targets and includes concrete actions. This process includes two kinds of activities: i) expert judgement and consensus, and ii) data and analysis, and is subdivided in four phases: i) planning and preparation, ii) visioning, iii) roadmap development, iv) implementation and revision. Figure 3 outlines this process, whose successful implementation requires 6 to 14 months according to [IEA 2010].



In [IEA 2010] it is suggested that "*expert workshops and consensus-building activities form the core of an effective technology roadmapping process*", and suggestions are given on how to include target setting, identifying technology needs and assigning actions. It is also suggested that such an activity should be conducted by experts that represent not only the different stakeholders, but also the different disciplines that relate to technology development, including technical experts, policy, economics, finance and social sciences. Good practices for TRM construction are then defined in [Londo 2013], based on a wide analysis of existing TRMs.

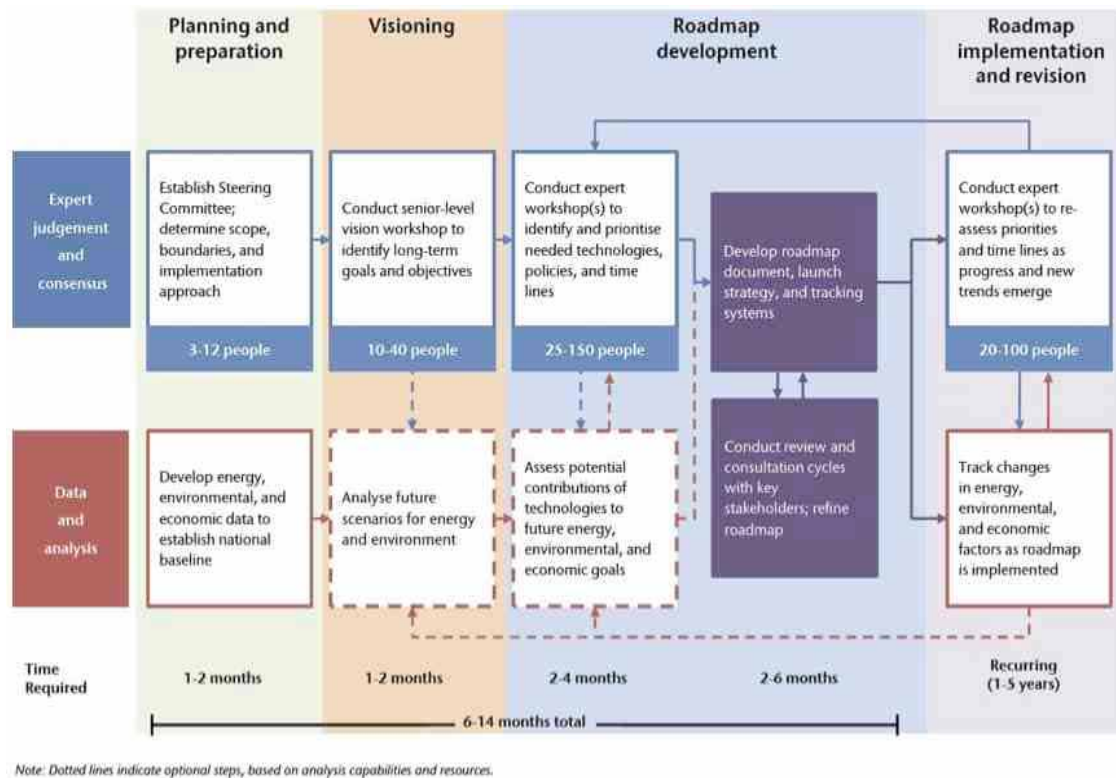


Figure 3: Overview of the policy-oriented roadmapping process proposed in [IEA 2010].

Finally, it is worth mentioning that detailed guidelines for the TRM construction process have also been developed by the Canadian Government [Industry Canada]. These guidelines are part of the Technology Roadmapping Initiative, an extended effort carried out jointly by the Canadian Government and industries since 1995. Although this initiative is mainly related to industry roadmapping, it also involves government policy.

In the following we give two examples of normative and exploratory roadmap construction.

4.2.3 EXAMPLES OF ROADMAPPING PROCESS

A normative roadmap

[Kerr 2013] presents a paradigmatic example of roadmapping for a normative, goal-oriented roadmap. In that case, the goal has been defined by the decision-making level, and consists of implementing the government's defence policy for improving and renewing the Royal Australian Navy. As a preliminary step, financial and technological constraints (e.g., practical applicability of the available technology) must be taken into account when defining methods and strategies to achieve the predefined goals. In this case study the constraints were:

- Funding issues: trade-offs between the operational needs of the military and the government's

budget constraints.

- Requirements issues: trade-offs between the government's budget constraints and the technology availability from industry.
- Maturity issues: trade-offs between the operational needs of the military and the technology availability from industry.

The normative approach for roadmap construction needed an overall top-down process, starting with the goals stated by the decision-making (political) level. This process is made up of two steps:

1) A **backcast** activity was conducted to plot the principal tasks, future roles and military capabilities required of the Navy in 2030. An end-state visual depiction of the maritime force elements was then generated using the strategic capabilities-based representation developed in [Kerr 2008] (see the block "End-state Capabilities" in Figure 5). We point out that the CyberROAD roadmap can not refer to clear, high-level goals defined by the EU, and thus the "required capabilities" from the EU are not available in our project.

2) Starting from this well-identified final state, a transition platform to desired state was realized (**path dependent** transition): the platform transitions of the various vessels (ships and submarines) was mapped, taking into account the path dependencies of the legacy fleet. Finally, the main projects to be conducted to deliver newly upgraded systems to in-service vessels was plotted over the medium-term to account for capability shortfalls/gaps until the newly introduced platforms obtain full operational readiness.

Figure 4 and Figure 5 show respectively the roadmap template and the final roadmap. The two steps above are described in more detail in the following, and are depicted in Figure 6.

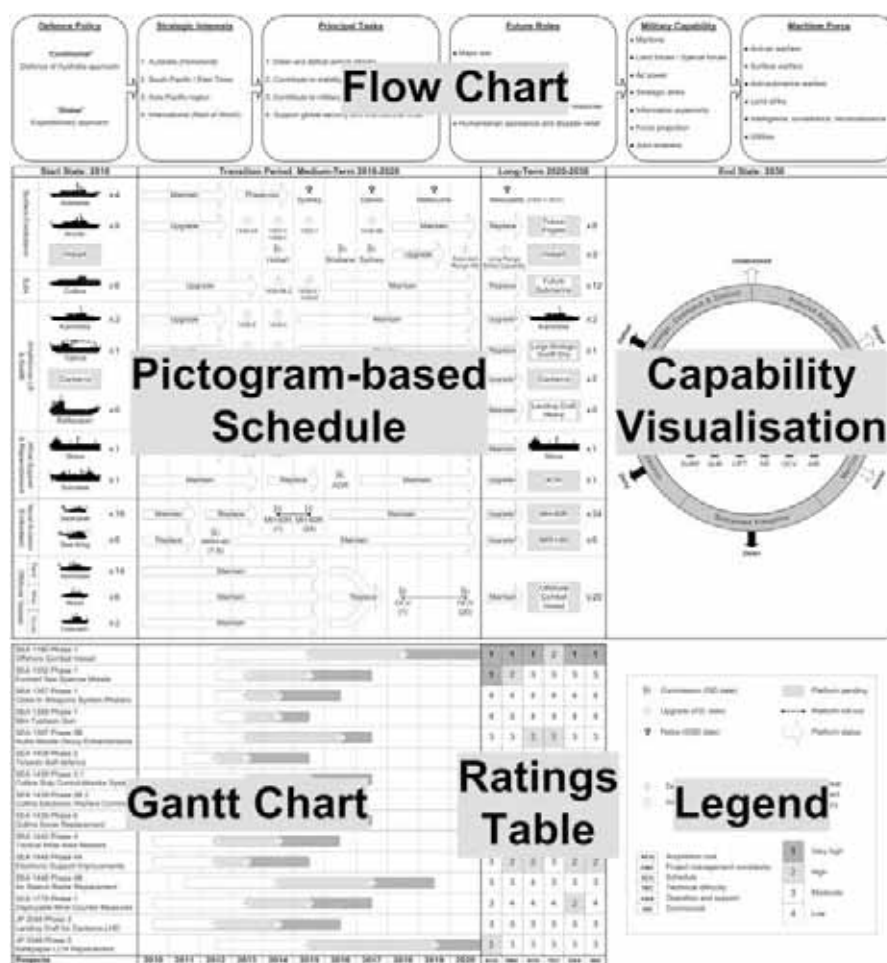


Figure 4: Template of the graphical representation of the roadmap in [Kerr 2013].



1) Backcast. This activity consists of describing a desirable future and of assessing how it could be achieved. The backcast must be (a) **normative** (the future is being chosen, not predicted), (b) **design-orientated** and (c) **sequenced**, as described below.

(a) *Normative backcasting.* The backcast begins with a definition of the future goals and objectives, which are plotted across six points in the top layer of the roadmap (the block 'Context' in Figure 5, see also Figure 6). Points 1-6 are respectively: the defence policy stance; the strategic interests; the principal tasks; the future roles; the military capabilities; the maritime force.

(b) *Design-oriented backcasting.* Backcasting is design-oriented because it is driven by an explicit image of the future. In this case study, the end-point is the end-state capabilities shown Point n. 7 in Figure 6. It represents the vision for the Navy's contribution to 'Force 2030' and defines the future warfighting elements, effects and complex product-service systems.

(c) *Sequenced backcasting.* Backcasting involves sequencing or reasoning, starting from the desired future end state and working back in time to the present to elicit what must be done to realise the vision. The sequencing part of backcasting starts at Point 7 in Figure 6, and works back through two pathways: Point 7 to 8 consider the fleet-level transitions that must take place to arrive at the Navy's end state capability vision; Point 8 to 11 considers the technological-based projects that must be delivered into the fleet during the interim. These pathways are focused on the new systems, i.e. the introduction of new naval vessels into service and breakthrough technologies, but the pathways related to the legacy systems should also be taken into account.

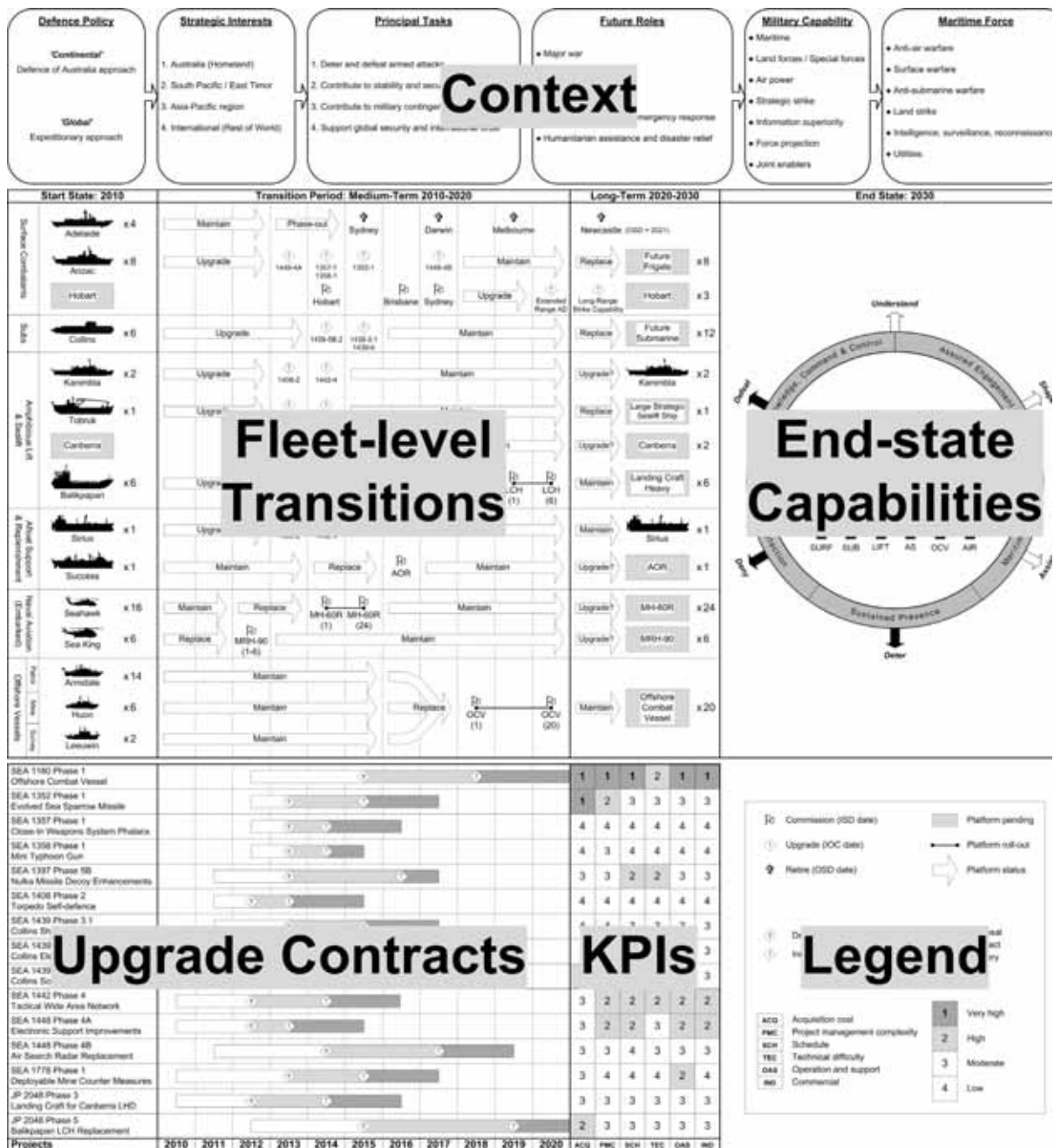


Figure 5: The graphical representation of the roadmap in [Kerr 2013]

2) **Path-Dependency:** the pathways related to the legacy systems. The future state of an organisation such as the Royal Australian Navy is heavily influenced by its current situation, so the path to build the new fleet must take into account the current state. In Figure 6 the path dependency involves Points 9 to 12. Point 9 to 10 considers the present day fleet as the start state and determines whether a particular class of vessel will be maintained, upgraded, replaced or phased-out. Point 11 to 12 considers the upgrade projects that will be necessary to sustain the operational capabilities and associated readiness levels of the systems on the older vessels.



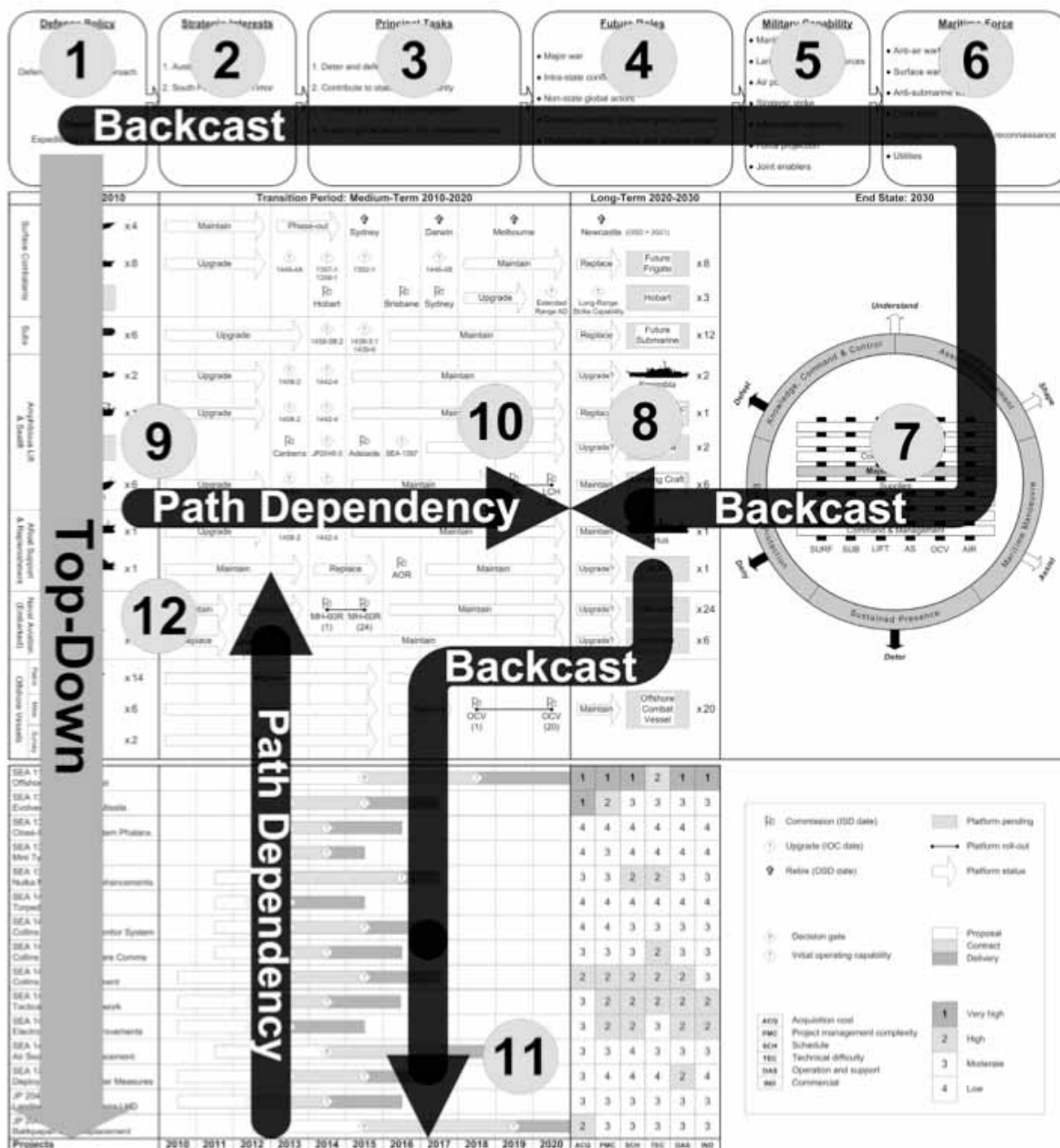


Figure 6: Sketch of the roadmapping process described in [Kerr 2013], with reference to the roadmap shown in Figure 5

An exploratory roadmap

In [Geschka 2013] an interesting example of a scenario-based, exploratory roadmapping process is presented. This case study focuses on fuel cells, but the used methodology can be generalized. As already mentioned in Section 1.2.1, according to [Geschka 2013] scenario-based roadmaps must take into account that many technologies are strongly affected by non-technical influencing factors (exogenous factors). In particular, such factors can be either direct (market factors like demand and competition, laws and standards), having an immediate impact on a product or a production process, or indirect (basic trends in society, politics and economy), as summarized in Figure 7.

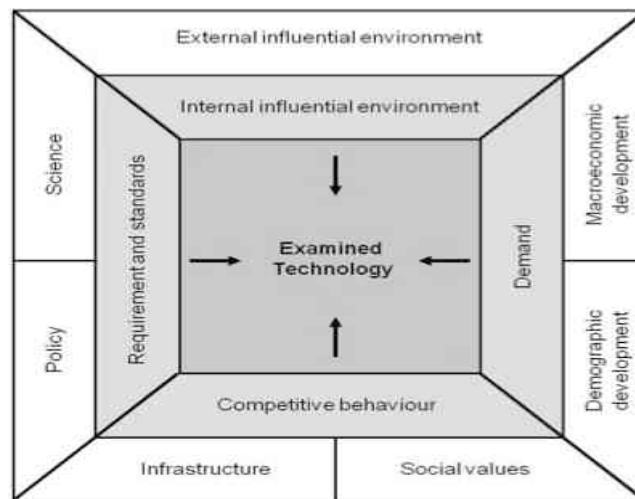


Figure 7: Input factors for scenario-based technology forecast [Geschka 2013].

Building a set of scenarios consists of three main steps:

1. Identification of exogenous influencing factors on the investigated topic;
2. Projections of the most relevant factors along with arguments for the projection (alternative projections are possible);
3. Combination of the alternative projections into *scenarios*, i.e., consistent bundles of projections.

The third step is achieved with the aid of a "consistency matrix": all projections are confronted with one another to assess whether they agree or are contradictory, according to a scale ranging from +3 (perfect fit) to -3 (completely contradictory). The combinations of highly consistent projections are selected, and a number of alternative scenarios are created.

The process of scenario-based, exploratory roadmap construction consists of three main stages shown in Figure 8, and is summarized below. Stages 1 and 2 refer to the basic principles, and Stage 3 refers to the development of the technology pathways.

	Stage 1: Technology analysis	Stage 2: Environment analysis	Stage 3: Roadmap development
Definition	<ul style="list-style-type: none"> • Definition of the technology under investigation • Identification of all part- and process technologies 	<ul style="list-style-type: none"> • Identification and structuring of relevant non-technical influencing factors on the technology under investigation 	<ul style="list-style-type: none"> • Identification of requirements on the investigated technology and all other elements of the technology complex aligned on the scenario pathways
Description	<ul style="list-style-type: none"> • Description of the present situation of all technologies in the technology complex 	<ul style="list-style-type: none"> • Description of the present situation and projections on the possible future development of all influencing factors 	
Analysis	<ul style="list-style-type: none"> • Impact analysis of the elements of the technology complex 	<ul style="list-style-type: none"> • Impact analysis of exogenous factors • Bundling and selection of consistent future scenarios 	<ul style="list-style-type: none"> • Consequences for the technology development and interdependencies between the elements of the technology complex
Result	<ul style="list-style-type: none"> • Description and analysis of the state of the art of the technology complex 	<ul style="list-style-type: none"> • Description of scenario pathways of the technology environment 	<ul style="list-style-type: none"> • Elaboration and visualisation of technology pathways

Figure 8: The process of scenario-based, exploratory roadmapping of [Geschka 2013].



Stage 1: Identification of the technology field. The starting point of the roadmapping process is a description of the state of the art of the considered technology, and of all the identified elements of the technology complex. Other aspects like legal regulations have to be taken into account as well. The description of the current situation is crucial for an exact definition of the technology under investigation.

Stage 2: Scenarios for the influential environment. The non-technical influencing factors should be identified and analyzed to develop an accurate picture of all interdependencies within the impact area, thus deducing the consequences for the technology. This is achieved in five steps:

Exogenous influencing factors. They include legal regulations, demographic development, availability of resources, market trends and changes in the competition pattern, as well as the requirements of users and consumers. It is important to select only those factors that have a direct impact on the technology. The more indirect the impact of the factors is, the more difficult it becomes later to deduce consequences and requirements for the technology.

Describing the state of the art. Next, the state of the art has to be described, projections into the future are developed. It is suggested in [Geschka 2013] that the number of projections per factor should not exceed three.

Scenario building. The alternative projections are compared with each other in a consistency analysis and grouped into consistent sets that form the scenarios for the non-technical impact area. For the roadmap development it does not make sense to analyse several scenarios: only one or two scenarios can be considered, selecting the most consistent one and perhaps the most “optimistic” one, to depict the decisions and measures that would lead to a desirable future situation. As a “counter scenario” the most pessimistic one could be chosen, in which decisions are postponed or certain features are not implemented.

Generating interim scenarios. Long-term scenarios should be divided in time sections, and interim scenarios are generated backwards to the present situation. The number of interim scenarios depends on the given time horizon, but for a differentiating roadmap two to three of them should be elaborated. To define their time span, one should refer to the company’s mid-term planning periods. Interim scenarios facilitate the later alignment within the strategy development.

Impact analysis. To identify the interdependencies within the technology complex and within the non-technical impact area, the factors and their relative influences are analysed by means of an impact matrix. All relations between the projections of impacting factors are reviewed in terms of whether they support or impede one another. This analysis facilitates identifying the most important “driver” factors, as well as the factors having a strong impact on the technology while being rather “driven” by the system.

Stage 3: Developing a roadmap. Detailed requirements on the technology complex and the product technology are derived from the previously established scenarios of the non-technical impact area. For each scenario, a corresponding technology roadmap is developed. To this aim, based on the development in the exogenous influencing area, the impact concerning the technology complex is described and specific requirements on the product technology are elaborated. The actual state of the product technology is described accordingly, for the interim point in time. This procedure has to be repeated for every interim scenario until the target one is reached. Therefore, for each interim scenario a “new” technology complex has to be described.

The development of technology paths starts with the present. The technology pathways are derived from the requirements. There is a sequence of different developments of technologies to fulfil these requirements. Differences in the possible development of the technologies may lead to a ramification of technology paths. In this case the solutions of each branch should be analyzed separately. If, for instance, the given forecasts concerning the availability of certain technologies are rather uncertain, a time-span should be provided.



As an example, Figure 9 shows a possible TRM for a fuel cell on the micro level. Each bar corresponds to a development level of the respective technology, drawn in chronological order. The white bars represent the technology development period. The grey bars mark the time-span during which the technology is available for utilization. The black bars show the period in which the technology is terminated (e.g., when it becomes obsolete). The arrows stand for structural relations between the technologies: a technology from which an arrow starts is urgently needed by the technology it points to). In addition, it is possible to visualize outstanding or trend-setting developments (projections) in the non- technical impact area (e.g., introduction of impacting laws). During the entire process of developing the roadmap, all new findings are constantly compared with the results that have already been produced, in order to attain a consistent picture of the development road. It is pointed out in [Geschka 2013] that the roadmapping process is not a linear one but rather a permanently iterative process. As the example above illustrates, such an approach might present certain benefits when studying issues of cyber crime and cyber terrorism that arise in an ever-changing landscape of information security.

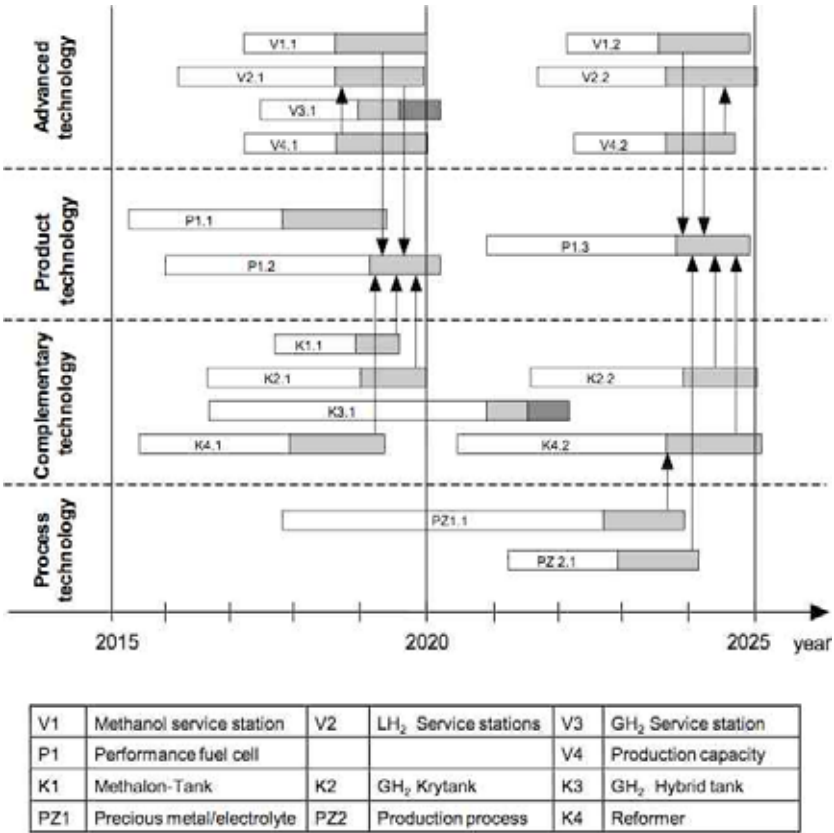


Figure 9: Example of a scenario-based, exploratory TRM [Geschka 2013], for a fuel cell application on a micro level.

4.2.4 DATA SOURCES, AND INFORMATION COLLECTION AND PROCESSING

One of the crucial, preliminary steps in the roadmap construction process is the definition of the data sources. In nearly all case studies, one or more sources among the following are used: experts in the domain of interest, stakeholders, scientific literature [Da Costa 2005; Codagnone 2007; Daim 2014]. In the case of technological foresight, the involvement of domain experts is crucial for defining the topic of interest, describing the present situation, and detecting, interpreting and projecting future developments [Geschka 2013]. Other statistical information gathered from

application-specific sources can also be used (e.g., patents [Choi 2013]). [Da Costa 2005] points out that information obtained from, e.g., Delphi studies or brainstorming workshops, has the advantage of originality whereas, e.g., on-desk meta-analysis of existing studies is less demanding in terms of resources.

In all the considered case studies the scientific literature is mainly analyzed by hand. The main problem pointed out in [Da Costa 2005] is that comprehensively mining the vast and increasing body of scientific literature and material is nearly impossible for human experts. On the other hand, developing text and data mining tools suitable for this purpose is still an open issue [Choi 2013].

Experts and stakeholders can be involved in different kinds of knowledge elicitation processes. To collect and organise information, experts can be directly involved in workshops (a concrete example of workshop organization is described in Section 2.2.7), can be interviewed independently on each other, or can anonymously participate and communicate in a Delphi study [Geschka 2013]. In particular, the **Delphi methodology** (see, e.g., [Kanama 2013]) is usually adopted to forecast technology trends in 20 to 30 years, giving a quantitative knowledge of the realization time and the importance level of technologies. Such a long time span requires the opinions of specialists in each field to produce a reliable result. The accuracy of the results depends on the scale of the survey and the number of respondents. A Delphi study consists of repeatedly conducting the same questionnaire survey with a large number of respondents, until their opinions converge. The survey process starts from the definition of the topics, related to possible science and technology achievements in the future, and of questionnaire items like the time of technological realization and the importance. Two main characteristics distinguish Delphi studies from traditional questionnaires. One is that, after the second questionnaire, the respondents are given feedback on the results of the previous one, to allow them re-evaluating their own answers by looking at the overall opinions trend. The other is the anonymity of the respondents, to avoid intentional bias resulting from recognizing specific respondents. A Delphi study can, based on predictions by scientists and other experts.

4.2.5 ROADMAP REPRESENTATION AND VISUALIZATION

The main characteristic of S&TRM methodology, is that "in comparison with other forecasting or foresight methods, [...] it includes graphic representations in which nodes (past, present or future states of the art in S&T development) are connected by links (causal or temporal relations) showing the nature, rate and direction of potential S&T developments from or towards those nodes" [Da Costa, 2005]. This allows S&TRM "to provide assistance to policy makers under information overload and time pressure to grasp effectively the most important elements and relations within a complex systems including scientific and technological, economic, political and social dimensions" [Da Costa 2005].

One of the great assets of graphical techniques is that they can convey large amounts of information in a small space and in an intuitive format. For these reasons, the most fundamental graphical depiction is the single-page, high-level strategic view that constitutes a 'strategic lens' on the problem that ensures that "the key issues are focused on" [Kerr 2013].

Typically, the architecture of a roadmap consists of two dimensions: the horizontal axis, which is most commonly a timeline, and the vertical axis, which consists of a number of layers that relates to different aspects of the problem. Each layer can provide an input to the next level. The minimum suggested number of layers is 3:

- Top layer is the '**purpose**' layer, which focuses on the 'know-why' dimension. It relates to the trends and drivers that govern the overall goals or purpose associated with the roadmapping activity.

- Middle layer is the ‘**delivery**’ layer, which focuses on the ‘know-what’ dimension. It relates to the tangible systems that need to be developed to respond to the trends and drivers (top) layer. Frequently this relates directly to the evolution of products (functions, features and performance).
- Bottom layer is the ‘**resources**’ layer, which focuses on the ‘know-how’ dimension. It relates to the resources that need to be gathered to develop the required products, services and systems, including knowledge-based resources, such as technology, skills and competences and other resources such as finance, partnerships and facilities. Basically, it could be a Gantt chart, that identifies the timing of the phases, enriched with other information [Kerr 2013].

The graphic displays of the roadmap are delivered with support documents. The graphic displays are more a synthetic tool, for the generalist view, whereas the documentation addresses the issues more in depth, for the expert view [Kerr 2013].

The generalist roadmap is developed first and is used to identify the areas where there are some knowledge gaps which can be roadmapped with a smaller granularity at a later stage. [Da Costa, 2005]

As mentioned above, [Kerr 2013] presents a paradigmatic example of roadmapping for a normative, goal-oriented roadmap (see Figure 5). In that case, the goal is to improve and renew the Royal Australian Navy in order to implement the Government’s defence policy.

The **purpose** layer consists of a flow chart scheme that shows a causal connection between the concepts. For instance, the key points of the flow chart are ‘Defence Policy’, ‘Strategic interest’, ‘Principal Tasks’, ‘Future Roles’, ‘Military Capability’ and finally ‘Maritime Force’.

The **delivery** layer is composed of two parts. On the right-hand side is the capability visualisation which is used to depict the end state vision for the Navy, that is, the salient aspects of the goal. On the left is the pictogram-based schedule which illustrates the fleet transitions from the start state (2010) to the end state (2030). The pictogram-based schedule is essentially a fleet plan that shows the in-service dates and out-of-service dates of the various vessels together with delivery of important technology enhancements during the in-service periods.

The **resources** layer has two interconnected visual elements: Gantt chart and ratings table. This layer aims to provide planners with high-level metadata relating to the upgrade projects over the medium-term as the legacy fleet is phased-out and transitioned to newer classes. The Gantt chart in the bottom layer identifies the timing of the phases (proposal, contract, delivery) for each project. Alongside the Gantt chart is a ratings table which provides a scoring mechanism for each of the projects against six attributes, namely:

Acquisition cost – What confidence do you have in the project cost estimate?

Project management complexity – How well do you understand the solution?

Schedule – How realistic is the schedule?

Technical difficulty – What is the technical complexity in delivering the solution?

Operation and support – What is the impact on the existing operating and support environment?

Commercial – What confidence do you have that industry can deliver the solution?

On the other side of the spectrum of possible roadmaps, [Beeton 2013] presents an exploratory roadmap. In this case-study, the expected outcome was to sketch a landscape of general needs of the sector of packaging. The main objectives were:

- To capture and structure the key trends and drivers facing the packaging sector over the next 10 years.
- To communicate detailed insights into the nature and implications of these trends and drivers, including identification of competitive threats and opportunities for innovation.
- To provide a framework to support strategic planning, decision-making and collaboration in the packaging sector.

The roadmap graphical template is shown in Figure 10. The horizontal axis (temporal dimension) of

the roadmap was set at a 10-year time horizon and was sub-divided into categories of short, medium and long-term. In addition to these horizons, the architecture categorized historical issues (i.e., events that have occurred in the past, but remained relevant) and issues that may occur beyond 10 years, which were classified as visions, predictions or aspirations.

Due to the specific application illustrated, roadmap layers differ from those showed by [Kerr, 2013]. The first layer represents the market trends and drivers that influence the development of the packaging sector (i.e., social, technological, environmental aspects).

The second layer represents products, services and applications. The sub-categories in this layer were derived from a model of the lifecycle of packaging.

The third layer represents technology, capabilities and knowledge that are available and emerging technologies that are directly related to the packaging sector. The technology layer was divided into two sub-categories of 'product' and 'process'.

The fourth layer of the roadmap architecture considers the development of resources that are not attributable to the other three broad layers. These resources are notionally considered to support the development of technologies and products, incorporating considerations such as capital, finance, skills, partnerships and supply chain interactions.

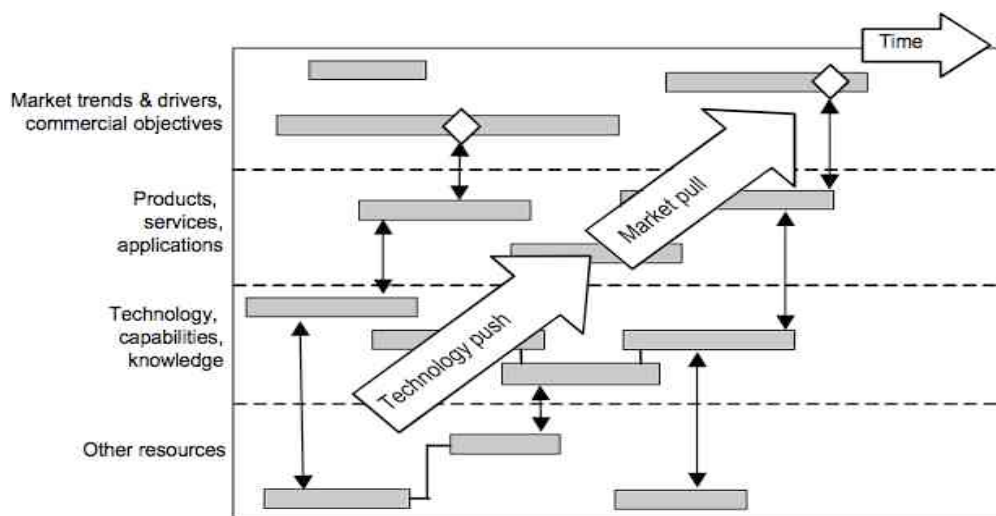


Figure 10: The roadmap template of [Beeton 2013].

A key objective in this process was to obtain a level of abstraction that enabled clear communication, whilst maintaining a sufficient level of detail. To facilitate this, a hierarchical approach was adopted, whereby the data was structured into two levels. The first graphic developed, shown in Figure 11, is a high-level depiction of the roadmap presenting the key points in the broad layers and sub-layers of the roadmap architecture.



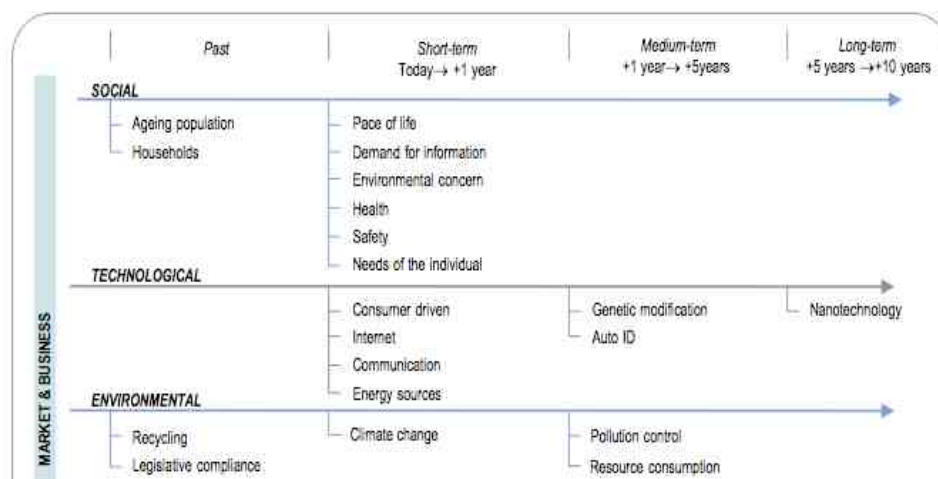


Figure 11: High-level view of the roadmap representation of [Beeton 2013].

The key aspects of Figure 11 are:

- It provides a succinct summary of the range of issues covered in the roadmap;
- It provides a clear depiction of the categories of abstracted codes created by the broad layers and sub-layers of the roadmap architecture;
- It illustrates the time horizons in which individual abstracted themes are believed to be most important.

A detailed graphic was then developed for each of the key points. For example, for the social aspect 'ageing population' the graphic could be the one in Figure 12. An example of the information presented in the graphical representations of the detailed insights, for one of the key points of Figure 11.

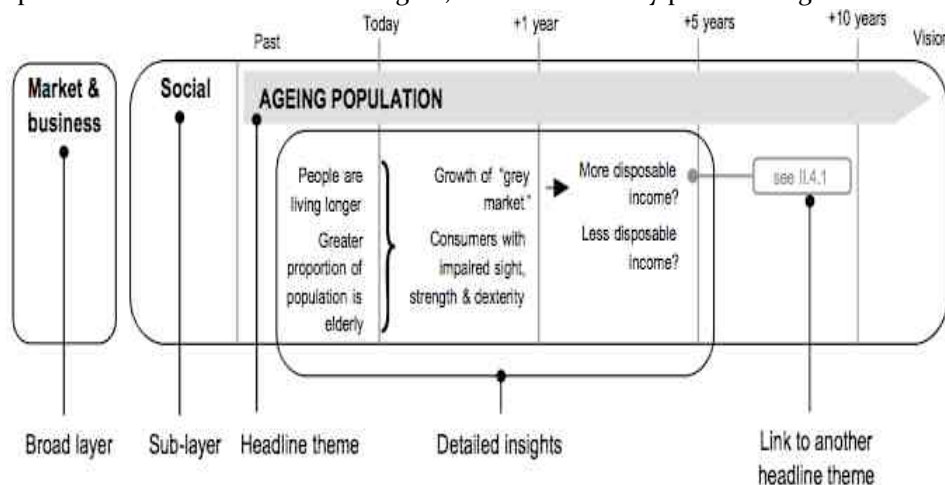


Figure 12. An example of the information presented in the graphical representations of the detailed insights, for one of the key points of Figure 11.



The key aspects of these illustrations are:

- The broad layers and sub-layers of the roadmap architecture in which the key point (abstracted code, in the paper) is placed are shown;
- The appropriate time horizons are emphasized;
- The relationships between certain key points are identified with arrows.
- Links to other key points are shown. The number of links included in the illustration is kept to a minimum as it was found that a greater amount increased the complexity of the graphic.

4.2.6 EVALUATION OF ROADMAP QUALITY

Ensuring the quality of a roadmap is a fundamental issue that has to be addressed early during the implementation phase [Da Costa 2005; Londo 2013].

Several suggestions and guidelines are reported in [Da Costa 2005], with a focus on S&TRM for policy intelligence:

- *"The ultimate evaluation of a foresight study" is defined as "whether the outcomes have been translated into actions and have triggered some changes within the client organisations".*
- *"The main characteristics of successful roadmaps are their clarity, relevance, focus on the information displayed in the graphics, and a clear synthesis and presentation of the core issues. Ideally, decision-makers can concentrate on what is relevant for the strategic decisions to be taken rather than being diverted by excessive detail".*
- It is suggested that the following key factors should be taken into account during the implementation phase: prioritising and selecting only the most relevant challenges/functions/technologies to be analyzed; focusing on some of the major societal challenges (human factors like economic, social, human and demographic dimensions), rather than being pushed by technology and technology developers; transparency of the roadmapping project (to be considered early in the definition stage), for ensuring the legitimacy of studies that may later be used to support major decisions in R&D policy; guaranteeing reliability and replicability (e.g.: *"To what degree would a roadmap be replicated if a completely different development team were involved in its construction?"* [Kostoff, 2001]); providing user-friendly outputs to avoid information overload.
- It is also suggested that peer review steps should be built early within the roadmapping process (e.g., during workshops with external experts), for validating the identification and the roadmapping of the key functions and enabling technologies.
- Finally, [Da Costa 2005] points out that, although policy intelligence roadmaps can be less "scientifically exact" than industry ones (that can usually exploit a much larger amount of resources), their value is identified in the vision at higher level of abstraction and in the inclusion of socio-economic and human factors, and their validation should be considered *"as much as an assessment of the relevance, a 'market testing' or a quality control rather than a pure scientific validation"*.

Relevant insights for policy intelligence TRMs are reported also in [Londo 2013], based on the analysis of about 200 existing TRMs (see above). Here TRM quality is evaluated in terms of six factors: *"the presence of a process description, a specification of stakeholders, clear (quantitative) targets, clear actions, a structured visual and a plan for updating of the TRM"*. [Londo 2013] finds that most of the considered TRMs *"do not satisfy several of these elements, and very few meet 5 or more of them"*, and in particular: *"clear visions, targets and actions are missing in almost half of the TRMs analysed. The other elements, process description, stakeholders specification, and visual representation, appear even less frequently. The least-present element is a plan for updating the TRM"*. Accordingly, a selection of good practices is given, based on several examples of existing TRMs.

[McDowall 2012] addresses the specific issue of identifying the right scope of a roadmap. This is especially relevant for technology transitions TRMs, where the most appropriate view of the future or transition timing may not be clear enough: whereas, narrow, prescriptive roadmaps are most effective in driving action, they tend to reflect dominant stakeholder interests and neglect alternative futures balance; on the other hand, less narrow TRMs run the risk of inaction from users due to uncertainty. A set of criteria is then defined to balance these objectives:

- Credibility: Is the roadmap based on sound analysis?
- Does the roadmap draw on the right breadth of expertise?
- Has the roadmap secured the participation and commitment of key actors in the innovation system?
- Does the roadmap adequately address the political, social and economic aspects of the transition?
- Desirability: Does the transition meet social goals established through democratic institutions?
- Does the roadmap give a clear account of the justification for the proposed pathway, with transparency in aims, process and who took part?
- Is the roadmap process inclusive and participatory?
- Utility: Does the roadmap effectively articulate a path forwards that can enable alignment around common goals?
- Is the roadmapping approach appropriate for the stage of innovation system maturity?
- Adaptability: Does the roadmapping process involve periodic reviews, updates and learning?
- Is the roadmapping process embedded in a broader institutional structure that enables reflexivity and learning?

Criteria for quality evaluation of policy intelligence S&TRMs are proposed also in [Jeffrey 2013] in terms of nine metrics reported below, subdivided into two groups. Each metric is given a score from one (low) to ten (high).

- Metrics assessing the TRM architecture and how it was prepared:
 - Author: Scored depending on the reputation of the author and who they selected to be a part of the TRM process (this is a traditional success factor for compiling a roadmap).
 - Target audience: Scored based on how well the roadmap addresses its entire target audience.
 - Roadmap message, effectiveness of delivery: Analyses a roadmap's message and how well it is delivered, taking into account format consistency and language.
 - Are the stakeholders adequately addressed? Measures how well, and how evenly, the stakeholders relevant to the roadmap are addressed.
 - Ease of use/method used: Measures how easy to follow the roadmap is for readers from a range of backgrounds.
- Metrics assessing the TRM results and whether its objectives have been achieved:
 - Status of suggested policies: Scored based on whether the roadmap's suggested policies have been implemented or are in the process of being implemented.
 - Citations and references: Scored based on the number of times the roadmap has been cited (highest weighting for citations by another roadmap or by government).
 - Technology: Scored based on whether the roadmap's technology recommendations have been, or are in the process of being developed.
 - Supply chain: Scored based on whether the roadmap's supply chain recommendations have been or are in the process of being implemented.

From the analysis of several case studies, evaluated according to the above metrics, some guidelines are elaborated for implementing a successful roadmap. Here we summarized them: 1) Having the right people/author in place; 2) Target audience involved as a key stakeholder; 3) Keeping the

roadmap “alive”; reviewing and updating it, and using it as an open line of communication with the target audience; 4) Well defined and evenly and effectively addressed target audience; 5) Clear goals and prioritised objectives to avoid trying to do too much; 6) Effective layout, structure and efficient use of visual graphs; 7) Focus on clarity and use of concise language; 8) Robust method for developing the roadmap.

It is worth quoting here the entire discussion about point 4: ***"It is important to have a well defined target audience. Having input from a wide range of stakeholders across government, academia and industry, ensuring that the roadmap targets all classes of stakeholder and striking a careful balance between a broad approach and a prioritised approach are all critical to evenly and effectively addressing all relevant stakeholders. This is closely linked with having clear defined goals and prioritised objectives to avoid trying to do too much. For a traditional roadmap, the target audience is usually the same company which is responsible for developing the roadmap. This is not the case for many multi-organisation roadmaps, which have to effectively and evenly consider a wide and diverse array of target stakeholders."***

The relevance of identifying the target audience of a policy-oriented roadmap is pointed out also in the eGovRTD2020 EU project, whose context is similar to CyberRoad: *"Since collaboration of different agencies at all government levels is a rather difficult process, proper planning and clear identification of the actors and their potential roles are crucial"* [Codagnone 2007].

A concise list of conditions proposed by several authors as necessary for producing high quality roadmaps is also given in a TRM literature overview, with no further elaboration [Carvalho 2013].

Finally, detailed specifications on how to evaluate and validate TRMs have been defined by the Government of Canada [Industry Canada], although they are mainly targeted to industries. These guidelines consider both shorter-term issues (TRM activities, outputs and reach, and its direct and/or immediate impacts) and longer-term impacts of the TRM initiative. Measures (mostly quantitative) for determining the achievement of each step in the TRM process are defined, as well as criteria for evaluating the participation of stakeholders (in this specific case, industries and government) and for monitoring and managing TRM projects.

4.2.7 EXAMPLE OF A ROADMAP OF INTEREST TO THE CYBERROAD PROJECT: EGOVRTD2020

The EU FP6 project "Roadmapping eGovernment Research - Visions and Measures towards Innovative Governments in 2020" (eGovRTD2020, January 2006 - May 2007) had the overall aim of constructing a policy-oriented S&TRM to identify and characterise the key research challenges, required constituency, and possible implementation models for holistic and dynamic governments in Europe and around the world in 2020 and beyond [Codagnone 2007].

A non-normative, long-term S&TRM approach was adopted, which addressed in a *holistic* way broad societal challenges, beside technological ones. An overview of this approach is shown in Figure 13, and was summarized in [Codagnone 2007] as follows:

- Current research (the state of play) and longer-term future needs (scenarios) are synthesised, and gaps in current research are identified.
- From the above results, several themes for future research in eGovernment are derived, which comprise the actual roadmap. Measures and actions as well as key actors - in research, ICT industry, consulting, and governments - are defined for these themes.
- By putting the proposed measures into a timeline, a roadmap for future eGovernment research is constructed to streamline the activities and developments of the field towards an intended future. The roadmap defines measures to take in research, development, demonstration, implementation, promotion and training, assessment, and standardisation.

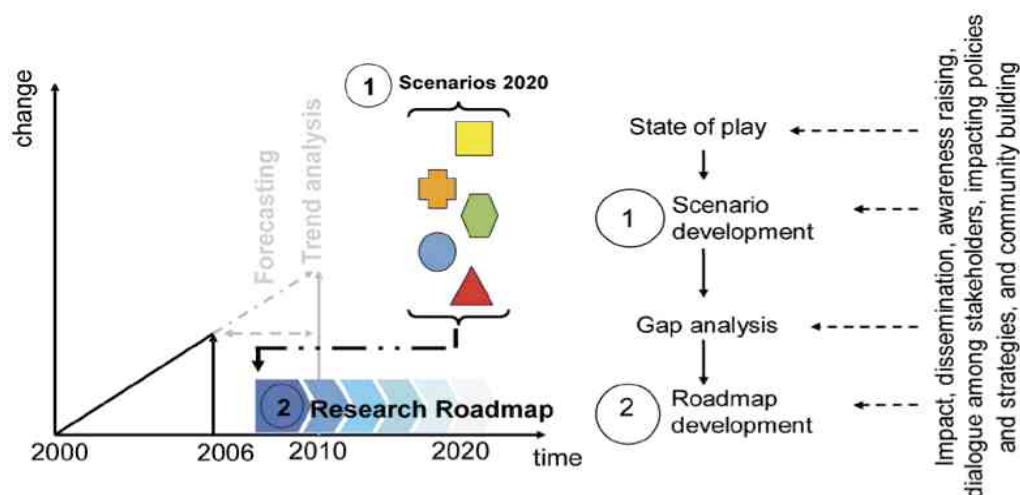


Figure 13: Overview of the eGovRTD2020 roadmapping approach.

Several hundreds expert were involved from governments, ICT industry and consulting, politics, and researchers, in regional scenario-building and roadmapping workshops, as well as in an online consultation. A final online survey to prioritise the research themes was completed by 380 experts. In the following we describe in more detail the two main steps of the above approach (**scenario building** and **gap analysis**), and the operational methodology adopted to implement it.

Scenario building is a technique for stimulating different perspectives and images on the *unpredictable* future by identifying complementary and/or contrasting alternatives, allowing one to better predict the long-term evolution of a certain domain. In eGovRTD2020 each scenario describes a coherent set of visions on a possible future, in a neutral way (no position is taken to value a "positive" or "negative"), without requiring a consensus about visions nor an agreement between different scenarios.

Scenarios were developed in **regional workshops** with the participation of experts from governments, ICT industry and consulting, and academia. The methodology used to develop scenarios and to extract relevant scenario aspects is shown in Figure 14. A workshop protocol and templates to guide the group discussions and to document the scenario elements were previously developed (see below).



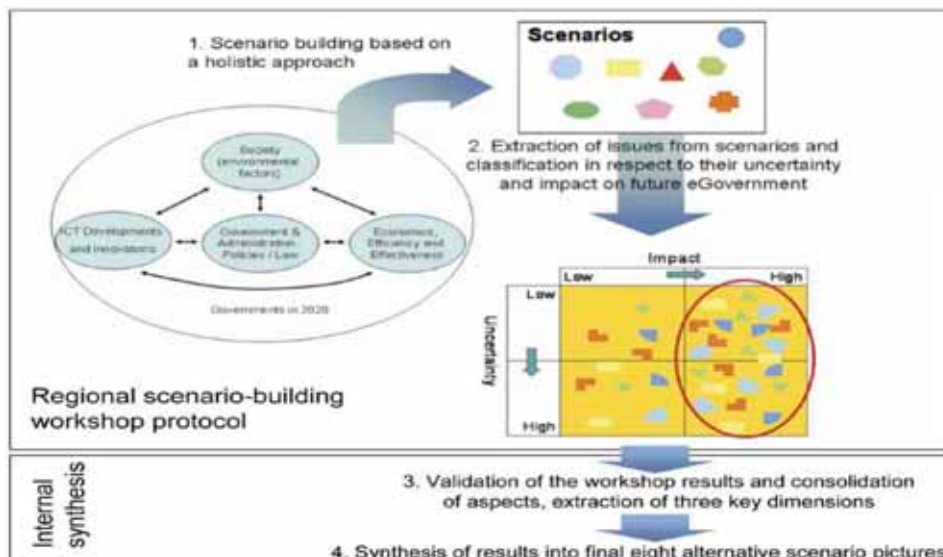


Figure 14: Methodology for scenario building in eGovRTD2020.

Experts were asked to extract important issues shaping the scenarios, as well as to assess their impact and likelihood, since a high uncertainty and high impact result in contradictory and alternative futures. A final set of scenarios was finally defined, covering the most important issues identified, and developing alternatives out of the uncertainty assessments.

Scenarios were constructed bottom-up. The issues identified were tagged with a topic of interest or a dimension, and were grouped into several categories (see Figure 15), which allowed to remove redundancies and to reduce the number of dimensions (resulting in 159 dimensions in 13 categories). Three key dimensions with their opposing extremes were then identified: the environment (will society, market and government be stable or disruptive in 2020?), the attitude towards government (trust or distrust in government activities), and the government scope (will governments provide all-inclusive services or concentrate on their core business and duties?). These dimensions were finally used in a top-down approach to create a final set of eight scenarios that formed the input of the subsequent gap analysis step.

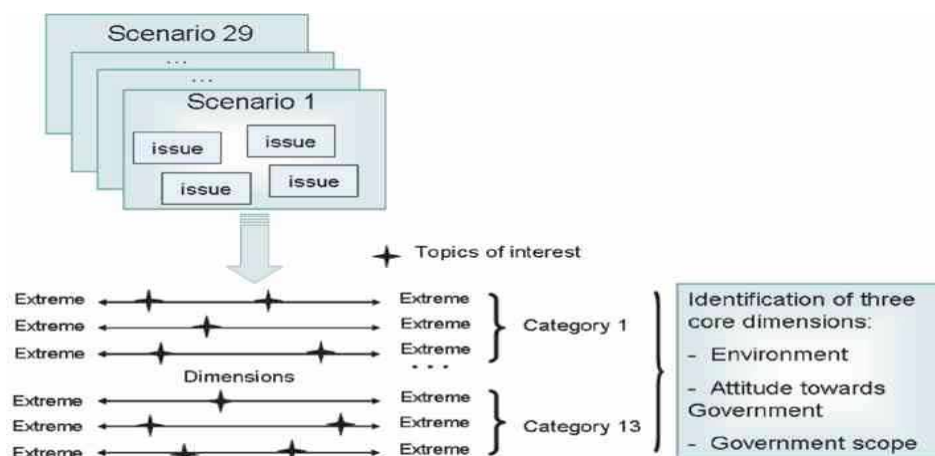


Figure 15: Characterization of scenarios in eGovRTD2020.



The protocol defined for regional workshops aimed at building scenarios (steps 1 and 2 in Figure 14) is the following:

1. Presentation of the project, of results from the state of play analysis, and of the scenario building approach.
2. Forming smaller groups of three to six participants with different expertise (distinct stakeholder groups and disciplinary background).
3. Group work: each group, under the supervision of a group moderator, was asked to develop one or more scenarios for eGovernment in 2020 using a predefined template.
4. Presentation of the scenarios and discussion in a plenary session.
5. Identification of key scenario issues (individual exercise): experts were asked to identify core issues of the scenarios presented, to assess them both in terms of impact on eGovernment in 2020 and the likelihood to happen in 2020 (uncertainty), and to place them in an assessment matrix (see step 2 in Figure 14).
6. Plenary discussion to resolve disagreements and to share a common understanding.

Gap analysis is used in traditional, normative strategic management approaches, to assess in a fairly objective and straightforward fashion the differences between the current status and the desired one. A different approach was adopted in eGovRTD2020, due to its non-normative nature. A gap was broadly defined as a mismatch between identified issues and future scenarios, e.g., an issue of current eGovernment research (identified in the state of play) that does not meet the emerging needs of future scenarios, or an issue that is not addressed by current research, or more broadly a discontinuity or an unknown. Such a definition of gap encompasses different issues than can emerge by a broad comparison of the state of play with the alternative possible futures elicited by the scenarios.

Previous approaches to gap analysis turned out to be not suitable to eGovRTD2020, e.g.: soft systems methodology (SSM); SWOT analysis methodology, used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in situations requiring a decision; ITPOSMO methodology (Information, Technology, Processes, Objectives and values, Staffing and skills, Management systems and structures, and Other resources, time and money), commonly used in eGovernment projects. Therefore, the revised methodology shown in Fig. [eGovRTD2020-GapAnalysis] was developed.

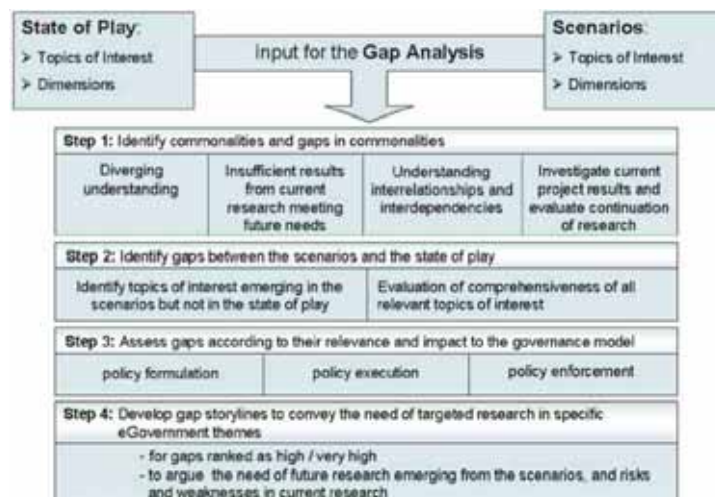


Figure 16: The gap analysis methodology adopted in eGovRTD2020.

The **operational methodology** adopted for the eGovRTD2020 roadmap construction, summarized

in Figure 17, is made up of four crucial activities:

1. Regional workshops with experts from governments, ICT industry and consulting, and academia, and an online consultation beyond the regional scale, to assess the scenarios and gaps identified, and to define key research themes for eGovernment, including indication of actions and actors to implement the research, as well as a time-frame.
2. Validating and consolidating the inputs from the regional workshops and the online consultancy, towards a research roadmap for eGovernment.
3. Exposing the extracted research themes to a wider group of experts through a focused consultation workshop, and integrating the results in the eGovernment research roadmap.
4. Assessing the importance of the research themes by a larger audience via an online survey, and prioritising them.

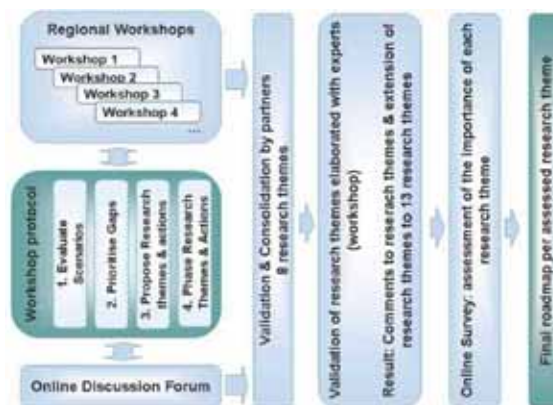


Figure 17: Overview of the eGovRTD2020 operational methodology

The aims and protocol of regional workshops and the online consultation were to: 1) Assess and comment the final eight scenarios; 2) Assess and prioritise the identified gaps; 3) Identify and develop research themes and actions; 4) Phasing the proposed research themes and actions.

An evolutionary approach was used to conduct the regional roadmapping workshops: the experience and feedback gained from each workshop were exploited for updating the materials and approach for the next rounds of workshops.

The results were synthesised and consolidated by the project consortium, which extracted eight research themes, actions and measures, and exposed them to experts via a validation workshop and an online survey, to assess the importance of each research theme.

Each research theme, the actions to take, the actors addressed and the time-span in which actions should be addressed were described in a structured form made up of three specific elements:

1. A detailed textual description of the research theme, including: a) The title of the research theme; b) A brief abstract; c) Three keywords; d) Key research questions.
2. A description of the research actions, means of actions, key actors and time-frame of action (a template is shown in Figure 18, left).
3. A roadmap chart indicating the actions in a time-scale (a template is shown in Figure 18, right).

The final eGovRTD2020 roadmap is made up of thirteen research themes, each with a number of activities and actors. Targeted decision makers at different levels (including the EU level, national level, ICT industry) can select the research related to the scenario hypothesis they favour. The eGovRTD2020 roadmap is thus a communication and awareness creation tool for relevant strategic

decision makers responsible for advancing society, government and industry developments.

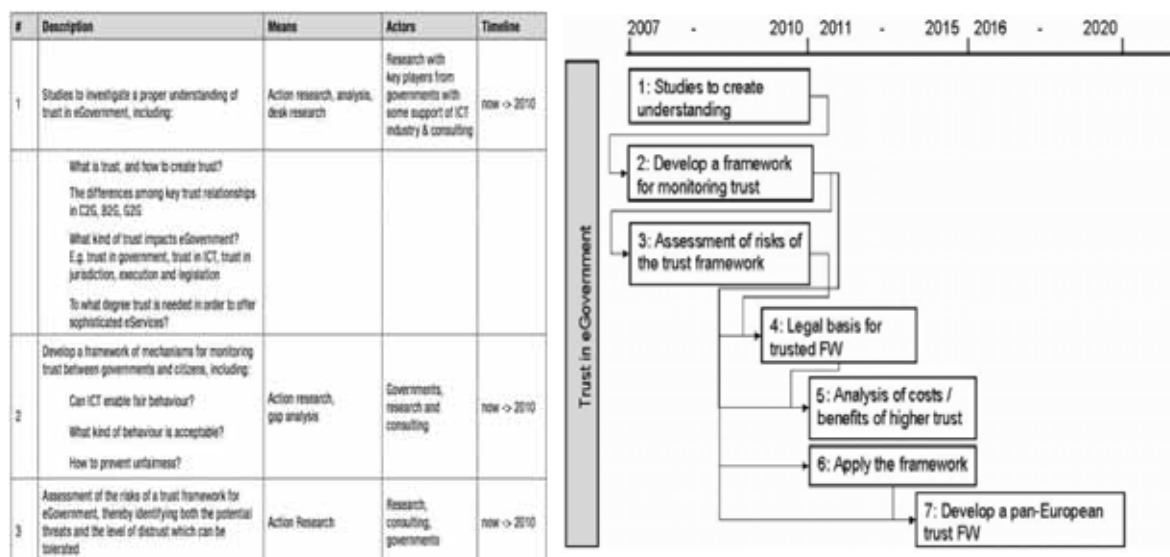


Figure 18: Left: a template for the description of the research actions, means of actions, key actors and time-frame of action, related to a given research theme identified in eGovRTD2020 (in this example: "Trust in eGovernment"). Right: a template of the roadmap chart indicating the actions in a time-scale, for the same research theme on the left.

4.3 FIVE KEY ISSUES FOR SCIENCE AND TECHNOLOGY ROADMAPPING

Based on the literature overview given in the previous section, in this section we identify five key issues related to the roadmapping methodology that have to be addressed during the WP2 of the CyberRoad project, according to the main goal of WP2 stated in Section B1.3.1 of the DoW: "define, develop and validate a coherent methodological framework" for the creation of the final roadmap. The key issues that have to be carefully addressed to guarantee a successful, high-level roadmap are:

- 1) Identification of the targets audience of the CyberRoad roadmap;
- 2) Selection of the data sources;
- 3) Definition of the techniques for creating the roadmap;
- 4) Definition of the techniques for roadmap representation/visualization;
- 5) Roadmap validation and quality assessment.

1) Identifying the target audience of the CyberRoad roadmap

As pointed out in the eGovRTD2020 EU project [Codagnone 2007] and in [Jeffrey 2013] (see Section 2.2), policy-oriented roadmaps are usually multi-organisation, i.e., they are not targeted to the same organization that produces them, and thus a wide set of target stakeholders from different domains has to be effectively and evenly considered. Precise target identification is therefore a crucial factor for the success of a policy-oriented roadmap, as the one that will be created by the CyberRoad project. The identification of the target audience should be strictly related to the choice of the type of roadmap to develop (normative, exploratory, hybrid, multiple roadmaps).

2) Selecting the data sources

By far, the three main data sources that are considered and used in S&TRM roadmapping are the scientific literature in the field of interest, the stakeholders, and the domain experts. Careful selection of the data sources is critical especially in policy-oriented roadmaps, due to their usually wide scope. In particular, policy-oriented roadmaps can require the involvement of hundreds of stakeholders and domain experts from different fields (not only from technology/science), as the eGovRTD2020 project clearly shows [Codagnone 2007]. Effective and efficient information/knowledge elicitation techniques have also to be identified. In the case of the scientific literature, a proper balance must be defined between manual analysis by domain experts and



Roadmapping methodologies and guidelines for information collection and assessment

Funded by the European Commission under the Seventh Framework Programme

automatic analysis, e.g., through data mining techniques, taking into account that no well defined and reliable enough solutions/tools exist yet for the latter. In the case of domain experts and stakeholders, suitable techniques should be defined to effectively organize and conduct workshops, meetings, etc., taking also into account the large number of persons involved, and their different fields of expertise.

3) Identifying the techniques for the creation of the CyberRoad roadmap

The S&T roadmapping literature review of Section 2.2 clearly pointed out that no single roadmapping methodology exists, even in the specific case of policy-oriented roadmaps. This is not deemed, however, as a negative aspect. Instead, as suggested in [Da Costa 2005] with reference to policy-oriented roadmaps, the roadmapping construction approach *"should be based on a light and modular process using a 'methodological toolbox' with different modules depending on the roadmapping areas, issues, context and objectives"*. Having said that, several suggestions, guidelines, best practices and detailed case studies can be found in the literature (the most interesting ones have been outlined in Section 1.2: [Da Costa 2005; Codagnone 2007; Londo 2013; Kerr 2013]), and can be exploited to guide the definition of a suitable roadmapping methodology for the CyberRoad project.

4) Defining the techniques for the representation/visualization of the CyberRoad roadmap

A concise and clear graphical representation is considered as the main characteristic of a S&TRM. This is a key issue especially for S&TRM targeted to the generalist view of policymakers, to allow them to effectively focus on the most important elements and relations in complex systems involving scientific, technological, economic, political and social dimensions. Similarly to roadmapping creation techniques, no single technique exists for constructing a graphical representation of a roadmap, but several guidelines and case studies are available in the literature, and can be exploited in the context of the CyberRoad project.

5) Validation and quality assessment of the CyberRoad roadmap

Our literature overview clearly pointed out that several issues must be addressed for ensuring a high-quality, successful roadmap, and that early actions must be carried out to this aim, since the roadmapping planning stage. Useful guidelines and best practices can be found in the scientific literature, and the most relevant ones have been summarized in the previous section. In particular, evaluating the quality of a roadmap during its construction is not sufficient: clear criteria and metrics have to be defined also to evaluate a roadmap during its *implementation*, in the considered time span.

Finally, we point out a relevant issue, among the ones mentioned in Section 1.2, to be addressed during the roadmap implementation phase, which is of particular interest in the context of the CyberRoad project. It is related to guaranteeing the roadmap reliability and replicability: *"To what degree would a roadmap be replicated if a completely different development team were involved in its construction?"* [Kostoff 2001; Da Costa 2005].

4.4 A FIRST PROPOSAL FOR THE CYBERROAD ROADMAPPING METHODOLOGY

First of all, it should be noted that a lot of technical reports, white and scientific papers, books have been published on the fight against cyber crime and cyber terrorism, providing the state of the art and candidate actions to limit the phenomena by technological, social and legal tools. Typically, they focus on the best practices in security, why they are not used or misused, and the way to promote the proper use of such best practices. Interesting enough, they lack the structure and vision of a roadmap. We think that this points out the added value that a well thought roadmap could have, so motivating the intrinsic value and the need of the development of a roadmapping methodology for the CyberRoad project.



In this section, we do a first proposal for the CyberRoad roadmapping methodology. This proposal wants to be a concrete basis for the work to be done in WP2 towards the definition of the operational CyberRoad roadmapping methodology. We start by illustrating the context of the CyberRoad project to point out the need of a roadmapping methodology. Then, we do our proposal for the CyberRoad roadmapping methodology. Finally, we propose the next steps to make towards the definition of the operational CyberRoad roadmapping methodology.

4.4.1 THE CONTEXT OF THE CYBERROAD PROJECT AND THE NEED FOR A ROADMAPPING METHODOLOGY

The project call

The CyberRoad project has been funded within the framework of the Work Programme 2013, under the theme “Security” and the research topic “*Developing a cyber crime and cyber terrorism research agenda*” (SEC-2013.2.5-1). The objective of this research topic, as stated in the call, is “*to develop a **research agenda** to provide concrete answers to the following issues:*

- *in what **categories** can we subdivide Cyber crime and Cyber terrorism?*
- *what are the major **research gaps**?*
- *what are the **challenges** that must be addressed?*
- *what **approaches** might be desirable?*
- *what needs to be in place for **test** and **evaluation**?*
- *to what extent can we test **real solutions**?”*

It is worth noting that there are multiple ways for the development of a **research agenda**.

As stated in the title of the CyberRoad project, as well as in the DoW, the project consortium decided that the production of the research agenda should take the form of a **roadmap**, namely, a process in which the identification of research gaps and challenges do not depend only on the analysis of past and current research activities, but also depends on:

- the forecast of future scientific and technological development and of the related social and economical evolution;
- the definition of goals (“*scenarios*”) that the activities of the roadmap are designed to get.

It is easy to see that addressing the above goals demands for a roadmapping methodology. In fact, the above two goals coincide with the goals of the two main types of roadmaps discussed in the previous section: exploratory and goal-oriented roadmaps.

The CyberRoad “Description of Work” document

The CyberRoad DoW is organized around 4 main WPs that act as the *main pillars* of the whole project. These WPs address all the issues that need to be taken into account for the creation of the research roadmap:

WP3 Social, Economic, Political, and Legal Scenario


WP4 Technological Scenario

WP5 Cyber crime

WP6 Cyber terrorism

While the last two workpackages tackle directly the main issues of the project, the first two WPs are aimed at the analysis of the environment where cyber crime and cyber terrorism take place.

By analysing the way in which the work has to be carried out in each of the above four WPs, it can be easily seen that they share the same basic structure:

	Roadmapping methodologies and guidelines for information collection and assessment
	Funded by the European Commission under the Seventh Framework Programme
	Page 38 of 65

- assessment of the state of the art, taxonomies and ontologies, and best practices;
- collection of stakeholders opinions;
- forecast of future and emerging scenarios.

If we look closely at these three basic modules of the structure of each WP, we can recognize the basic ingredients for the creation of a roadmap as outlined by the overview of the previous sections:

- a snapshot of the actual scenario based on data, documents, experts' opinions (*where we are*)
- the possible goals of the roadmap, i.e., the scenario as it ***might*** be according to the actual trend in the case of exploratory roadmaps (*where we could end up*), and the scenario as it ***should*** be in the case of normative roadmaps (*where we should go*)

Therefore, the two tasks that are included in each of the WPs from 3 to 6, namely, the assessment of the actual scenario, and the gathering of stakeholders' opinions, have the goal of assessing *where we are*, and *where we should go/could end up*, which are roadmapping tasks.

Therefore, the accomplishment of the above tasks of the project DoW demands for a roadmapping methodology. In fact, all the tasks of the DoW are common roadmapping activities.

The coordination and harmonization of the activities across all the WPs is done by **WP2** (Scientific Coordination WP), which acts as the *backbone* of the project. The activities of WP2 span all over the duration of the project, as they are aimed to *define, develop and validate a coherent methodological framework and pilot-testing used in this project*. In particular, the main goal of **Task 2.1** is to define the methodological framework, while **Task 2.3** will *supervise and harmonize the work of WP3, WP4, WP5, and WP6 on the basis of the guidelines developed in Task 2.1*. Accordingly, WP2 should specify and implement the CyberRoad roadmapping methodology. In the next section, we outline a first proposal for this methodology.

4.4.2 A PROPOSAL FOR THE CYBERROAD ROADMAPPING METHODOLOGY

First of all, we propose three main guidelines for the development of our roadmapping methodology. The CyberRoad roadmapping methodology should:

- leverage on the **best practices** described in section 2.2;
- address explicitly the **5 key issues** described in section 2.3;
- provide an **operation tool** to supervise and coordinate the work of all WPs for the creation of a high-quality roadmap.

These guidelines should allow the project consortium to claim that the final roadmap has been developed by a methodology carefully designed that exploits the best practices on science and technology roadmapping. This should also guarantee the quality of the final roadmap and its concrete impact on the EU research agenda against cyber crime and cyber terrorism.

WP2 (Scientific Coordination WP) should guarantee that the above guidelines are properly used during the execution of the project.

According to the above three guidelines, we propose a roadmapping methodology based on three phases:

- Roadmap preparation**
- Roadmap implementation**
- Roadmap validation and evaluation**

In the following, we describe each of the three phases, pointing out how they are related to the WP tasks and take into account the above three guidelines.

Phase 1: Roadmap preparation

The preparation phase should address the following issues:

1. Identifying the **targets** of the CyberRoad roadmap
2. Identifying the **goal & scope** of the roadmap: *normative, exploratory, hybrid*.
3. Selecting the **data sources**
4. Identifying candidate techniques for the **creation** of the roadmap
5. Identifying candidate techniques for the **representation/visualization** of the roadmap

The above issues can be revised further in the next phases but it is important that well-thought decisions are made during the preparation phase.

The preparation phase should focus mainly on the issues 1, 2 and 3. Issues 4 and 5 should be discussed in preliminary way during the preparation phase and addressed mainly during the implementation phase.

The identification of **targets** (end users of the roadmap and stakeholders) should be the first task to be accomplished in **Task 2.3** (Supervision and harmonization of WPs work). As the overview of previous work on S&TRM pointed out: ***it is very important to have a well-defined target audience from the beginning of the roadmap creation***. Especially for roadmaps like the one of the CyberRoad project that have multiple targets and stakeholders across government, academia and industry.

The choice of targets is also strictly related to the creation of the Liaison Database (**Task 7.2 of WP7**) and to the representation/visualization techniques used to convey all the roadmap information to the target groups.

Proper tools should be defined for a motivated choice of the targets. The advisory group should be involved for the decision. The identification of targets should be done in task T2.3 of WP2 by regular online meetings and exchange of documents.

The other fundamental decision of the preparation phase concerns the **type of roadmap**. As we saw in the previous sections, roadmaps can be *explorative, normative (goal oriented)* or *hybrid*, and the decision on the type of roadmap strongly influences all the following phases of the roadmap creation. As an example, this decision also influences **Task 7.2** (Liaison database), i.e., the definition of the **targets** of the roadmap, as the goal of this task is to define a database of the final recipients of the roadmap.

A *normative* roadmap implies the clear definition of the roadmap goals. Such goals should be provided/supported by the opinions of end users, stakeholders, policy-makers, and supported by available data on cyber crime and cyber terrorism (e.g., data of the Cyberdefcon observatory: <http://globalsecuritymap.com>). The decision for an *explorative* roadmap implies the creation of **scenarios** to explore (**scenarios building**). As an example, the goal of a normative roadmap could be to reduce the average cyber crime levels in Europe to the minimum levels reported for some countries (see <http://globalsecuritymap.com>). A scenario to be explored for an explorative roadmap could be the one of the continuous expansion of the internet of things and people and its effects on security and privacy on EU citizens.

Given the complexity of cyber crime and cyber terrorism phenomena, the possibility of **hybrid** roadmaps and **multiple** roadmaps should be also considered.



The use of three main **data sources** has been planned in the DoW: relevant documentation in the field of interest, stakeholders' opinions, and domain experts' opinions. The project consortium has been created to cover a wide spectrum of expertise and stakeholders from different EU countries, so that much of the data should be already available (they can be collected by the partners themselves), or can be collected by exploiting the network of contacts of each partner.

The use of **additional data sources** should be considered carefully in the preparatory phase.

The selection of additional data sources should take into account:

- the intrinsic value of data for the development of the roadmap;
- the way for the exploitation of data and the manual/(semi)automatic processing techniques requested;
- the availability of sources that can provide such data.

The selection of data sources and the harmonization of the methodologies for data collection and measurement are the core of the activities of **Task 2.1**.

The preparation phase should also consider the selection of additional **domain experts** outside the project consortium to define the state of the art, the scenarios, and the goals of the roadmap.

The above tasks should be done in task T2.3 of WP2 by regular online meetings and exchange of documents. Particular attention should be given to the choice of the type of roadmaps and the selection of additional data sources.

In answer to the above we have defined a concept to be used during the roadmap preparation.

We have called this concept 'The CyberROAD Evidence-Based Practice Triad', that provides practical direction from which to begin the roadmap preparation. It incorporates the three main guidelines laid out in 2.4.2 above.

As well this initiative addresses points 1 & 2 of the Phase 1 Roadmap Preparation and provides direction for points 3 to 6.

The concept called 'The CyberROAD Evidence-Based Practice Triad' wants to stress the fact that the CyberRoad roadmap should be based on reliable and carefully assessed experimental data and practical evidences.



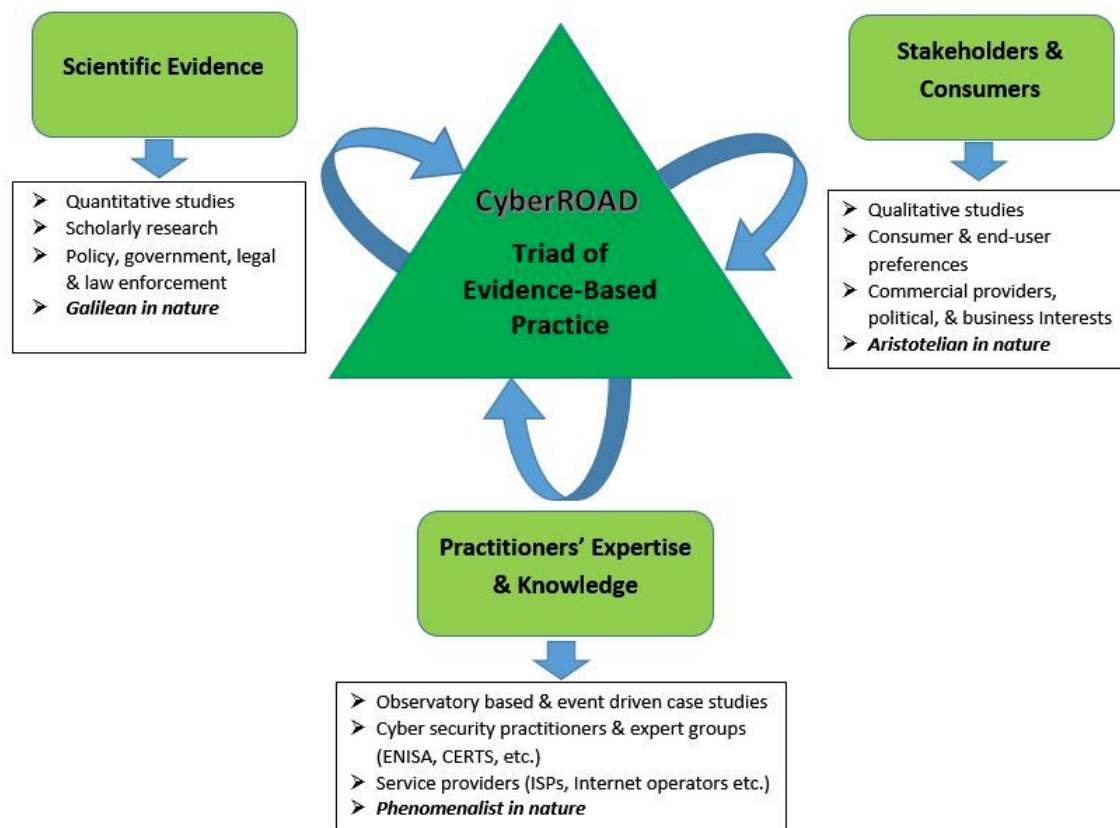


Figure 19: The CyberROAD Evidence-Based Practice Triad

The CyberROAD Evidence-Based Practice Triad

The Triad is based on tried and tested models used in many other fields and industries, for example in health care, and translates well for CyberROAD purposes.

The diagram illustrates how the use of the best scientific evidence (Galilean), integrated with observatory based & event-driven case study experience (phenomenalist), and incorporating consumer values, political and commercial preferences (Aristotelian) results in a pragmatic and flexible framework which can be molded to fit all the needs of the CyberROAD project. Using the model would provide impetus and clarity at the start of the project, which is essential for formulation of the preparation work. The advantage of this type of model is its flexibility and range of possible applications. It can be used as a basis of the roadmap and for exploration of the pertinent questions such as who, what, why, how and when, fit to this model and for the exploration of a number of alternative themes. For example, observatory and data sources fit the case study area while data source providers are collectively called 'Practitioners & Experts'.

Further, an evidence-based model will equip the project with supporting metrics which should be looked upon favourably when the policy makers decide if resultant research should follow.

Phase 2: Roadmap implementation

The **implementation phase** should lead to the construction of the roadmap, and consists of collecting, synthesising and validating the information, and representing the roadmap with graphic displays associated with support documents.

This phase is based on the output of the preparation phase in terms of:

- **targets** of the roadmap;
- **type of roadmap** (*normative, exploratory, hybrid*);

- **data sources.**

Depending on the above outputs, the implementation phase should address the following issues:

1. **Collecting the data** to use for the creation of the roadmap
2. Identifying the specific techniques for the **creation** of the roadmap
3. Identifying the specific techniques for the **representation/visualization** of the roadmap

It is easy to see that the choice of the specific techniques above strictly depends on the choice made in the preparation phase. In the following, we outline the general features of the tasks to carry out in the implementation phase.

Data collection

One the data source already identified in the project DoW is stakeholders' opinion. Data collection from this data source will be carried out by interviews with questionnaires. The definition of questionnaires is part of WP2. Two types of questionnaire can be considered:

- questionnaires aimed at surveying current scenarios, the foreseen trend and the present and future impact of cyber crime and cyber terrorism (useful for explorative roadmaps);
- questionnaires aimed to collect opinions and views of experts and stakeholders on the goals of the roadmaps (useful for goal-oriented, normative, roadmaps)

For example,

- **WP3** could focus on the target scenarios for legal, economical and social aspects: which kind of legislation we should have in place? Which kind of education should be given to citizens in order to raise their awareness on the use of the new technologies? Should regulations be negotiated with IT companies so that their product are compliant with such regulations? (see, for example, the “Cyber Essentials Scheme” in the UK)
- **WP4** could focus on the scenarios of technological evolution. Given the trend of evolution of emerging technologies, which features would be desirable so that they can be safely used and accessed by ordinary citizens? Issues related to the so-called “usable security” should be addressed.

It is mandatory that the goals are clearly defined using quantitative measures so that, if the roadmap is adopted, the progress can be verified.

Thus, the opinions that are sought with this questionnaire should reflect opinions on how security and privacy should be defined in the future. On the basis of this definitions, and taking into account the trend in the development of new technologies, it will be possible do depict future scenarios of the cyberspace as it should be.

The Triad model supports this supposition through the use of evidence-based data to challenge the status quo.

To describe how this could work we will use an example of a widely held belief within the field of cyber security, namely that anti-virus is the best way of protecting computers from viruses. Using the triad model, we would look at the available data to see if this is actually the case. In actual fact, the data would probably not support this widely-held belief as anti-virus is, by nature, reactive, or in other words, only acts on known viruses and, therefore, useless against new viruses.

Using the triad model, the current practice would be questioned, the evidence examined and the situation re-evaluated. The re-evaluation would take into account new research, case studies and qualitative analysis in order to identify the possible solutions using the collaborative influence of the three sectors. An understanding of how to face future scenarios will only evolve once the current status has been re-evaluated using rigorous examination and with appropriate questions.



Data collection should be also carried out by the organization of workshops. Workshop are aimed to discuss relevant issues in cyber crime, cyber terrorism and the related social, legal, and technological issues, so they should be focus on the relevant challenges, and on future scenarios. In other words, they should not be seen as the usual scientific or technological conferences, where researchers present their contribution to the advance of the state of the art. Rather, they should cover more fundamental issues, so that help defining the start and end points of the roadmap, as well as the milestones for travelling the path from the actual scenario to the emerging scenarios. Workshop planning is already underway, as stated within the D7.1 deliverable (“Dissemination Plan and Calendar of Activities”). Three CyberRoad Workshops are envisioned, targeting the relevant stakeholders, the academic community and the general public.

Techniques for the creation of the roadmap

The choice of the specific techniques for the creation of the roadmap depends on the choice of the type(s) of roadmap(s) done in the preparation phase.

However, according to the best practices illustrated in section 2.2.7, we propose that the creation of the roadmap is based on the **building of scenarios**, both for normative and exploratory roadmaps. Each scenario should describe a coherent set of visions on current and future situations of interest for the analysis of cyber crime and cyber terrorism.

WP3 and WP4 are expected to describe sets of possible **starting/current scenarios** (the state of play), as they are aimed to describe the current SEPL (Social, Economic, Political, Legal) and technological scenarios behind cyber crime and cyber terrorism.

WP5 and WP6 are expected to describe sets of possible **starting/current scenarios** (the state of play) for cyber crime and cyber terrorism.

WP3, WP4, WP5, WP6 should describe sets of possible **ending/target scenarios** for normative roadmaps and/or **future scenarios** for exploratory roadmaps. WP2 should rank and select the scenarios to be used and analysed for the roadmap creation.

WP3, WP4, WP5, WP6 should also describe **intermediate scenarios** and the techniques to create the **path** connecting starting/current and ending/target scenarios.

WP2 (in particular T2.2) should perform the so called **gap analysis** (section 2.2) to assess in a fairly objective and straightforward fashion the differences between the starting, intermediate, and ending/target scenarios, in order to identify the research gaps and their priorities. To this, T2.2 of WP2 will develop a risk assessment methodology.

Techniques for the representation/visualization

The goal of Task 2.4 of WP2 is to identify the most effective way to communicate the produced roadmap. Such a representation should be able to convey in a simple way the complexity of the work carried out within the project that involves a large number of experts, and stakeholders, as well as addressing different research topics from different perspectives. In particular, the representation of the roadmap should clearly show:

- the research issues identified in the WPs from 3 to 6
- the interdependencies among the different WPs
- the research priorities identified by Task 2.3
- the timeline of the roadmap



- the effort needed in term of people and organizations involved, costs, etc.
- the intermediate goals of the milestones

A starting point could be the classical representation with two dimensions (section 2.2): the horizontal axis as timeline, and the vertical axis consisting of a number of layers that relates to different aspects of the problem. Each layer can provide an input to the next level. According to the state of the art, the minimum suggested number of layers is 3:

Top layer is usually the '**purpose**' layer, which focuses on the 'know-why' dimension. It relates to the trends and drivers that govern the overall goals or purpose associated with the roadmapping activity.

Middle layer is the '**delivery**' layer, which focuses on the 'know-what' dimension. It relates to the tangible systems that need to be developed to respond to the trends and drivers (top) layer.

Bottom layer is the '**resources**' layer, which focuses on the 'know-how' dimension. It relates to the resources that need to be gathered, such as technology, skills and competences and other resources such as finance, partnerships and facilities.

The starting point could equally be in the 'triad' format as detailed above or other visual representation that will be considered suited to convey the main message that the definition of the roadmap aims to convey (e.g., <https://gephi.github.io/images/screenshots/preview2.png> provide an alternative graphical representation). The decision will be carried out during the second year of the project.

Phase 3: Roadmap validation and evaluation

This phase will be carried out with the help of the advisory board, which has been established as an external body to evaluate the products of the project.

The roadmap should be evaluated according to several criteria. For example,

- **completeness** of the data sources considered, the issues addressed, the panel of experts and stakeholder involved in the process.
- **feasibility** of the implementation of the roadmap in terms of the final and intermediate goals, the estimated effort and the external dependencies.

The set of criteria to use for the validation and evaluation of the roadmap should be defined with the advisory board and the stakeholders. Validation and quality assessment criteria must rely on quantitative measures. For example, what is an acceptable level of cyber crime and cyber terrorism activities? What is the temporal horizon that we can set to attain these goals?

WP7 could provide some quality measures related to dissemination of security awareness, for example: number of scientific publications arisen from the consortium (Impact Factor); number of backlinks talking about the program in blogs, magazines, ...; number of policy makers reached in dissemination activities.

The consortium should also perform a self-evaluation for each of the previous phases of the roadmap creation (preparation and implementation).

As pointed out in the previous sections, in order to have a solid background of the cyber security problem space and to proceed to the research of a roadmap for cyber security research activities, it is necessary to proceed to define two preliminary aspects:

- definition of an **ontology** and a methodology to treat this kind of problems, and
- definition of **guidelines** to conduct information collection and assessment

The following sections present a brief overview of the current cyber security panorama, in terms of actors and drivers of cyber crime / cyber terrorism, and the motivations behind them. The actual and potential targets of the attacks are identified and the general reason for cyber security is deduced. The current situation of cyber security facilities is analyzed and gaps and potential deficiencies are identified. Eventually, the methodology followed to define an ontology is presented, and the ontology is defined accordingly.

5.1 CYBER SECURITY PANORAMA

The explosive growth, complexity, adoption and dynamism of cyberspace that have enhanced social interaction and expanded our ability to productively utilize our environment have also introduced new adversarial threats and challenges to our society. Cyber crime, cyber terrorism, adversarial state-sponsored activities, and so on, are all exemplars of malevolent attributes of cyberspace. Mitigating these malevolent attributes requires an agile, legal and ethically compliant, interdisciplinary and scientifically-based research in order to develop an R&D program in cyber security. [Asgher 2013]

The cyber security research challenge over-all resides within a particularly complex area, being at the intersection of behavioral sciences, formal sciences and the natural sciences. As stated, cyber space includes a significant adversarial component which has led to a view, by the scientific community, that the science of cyber security is, in fact, a “Manichean science,” a science in the presence of adversaries, the core components being operations research, cybernetics and game theory. Consistent with this perspective are “nature inspired” approaches that draw upon analogies arising from immunological and biological systems. Other areas that could usefully inform a science of cyber security include cryptography, formal reasoning, machine learning and composition. [Asgher 2013]

To support information exchange and contextualization of the cyber crime and cyber security domains, it is useful to define an ontology that can be useful for research activities in the field. In the following sections, the most important concepts and characteristics of the cyber crime and cyber security are identified, analyzed, grouped together and presented.

5.1.1 THE DRIVERS AND ACTORS OF CYBER CRIME

To identify the main actors and drivers behind cyber attacks, current and potential threats are reported in Table 1 [ICSJWG 2011]:


	Roadmapping methodologies and guidelines for information collection and assessment
	Funded by the European Commission under the Seventh Framework Programme
	Page 46 of 65

Table 1: Actors of cyber crime / cyber terrorism

Actors	Motivation	Goals	Targets	Types of attack
Criminal and espionage groups, organized crime	Monetary gain, financial reasons, ransom	identity theft, online fraud, extortion, acquire intellectual property and know-how	Industry, finance, government	spam, phishing, spyware/malware
Insider (including employees, outsourcing vendors, contractors, business partners)	Money, vengeance, stalking, unintentional	damage target system, steal data	Industry, finance, government	unrestricted access, malware, inadequate policies and procedures
Phishers	Monetary gain	steal identities and information	Industry, finance, government	phishing schemes, spam, spyware/malware
Spammers	Monetary gain, reputation	sell products, attacks	Industry, finance, individuals	email spams, phishing schemes, spyware/malware
Malware (virus, botnets, spyware)	Espionage, vengeance, money	attacks of various nature, infect other machines, steal information, attack privacy	Industry, finance, individuals (files and drives), testing environments	spyware/malware (viruses)
Terrorists	Subversion of the current status quo through violent actions (can involve destruction in order to broadcast effectively a possible ideology or a political point)	threaten national security, cause mass casualties, weaken economies, undermine public morale and confidence	Critical infrastructures, government	phishing schemes, spyware/malware
Military	Achieve a political objective	Take down a specific target, cause distraction at the enemy	Military, Infrastructure, Communication,	Malware, Backdoors, Zero-Day Exploits
Intelligence Agency	Information gathering, strategic advantage	Collect all kind of information of friends and enemies that might be useful in the future	Government Agencies, Companies with a strategic value, NGOs	Passive eavesdropping, insiders, custom malware, backdoors, exploits

5.1.2 REASONS BEHIND CYBER SECURITY

The fundamental motivations behind the necessity of have cyber security are deduced [Consoli 2014]:

- improve technological security to serve our life
- protect privates, firms, institutions and governments
- safety of systems, safety of life

5.2 CYBER SECURITY ONTOLOGY

5.2.1 WHAT IS AN ONTOLOGY?

In the Information and Computer Science field, [Gruber 1993] shortly defined the term **Ontology** as “a specification of a conceptualization”.

More extensively, an Ontology is a specification of a representational vocabulary for a shared domain of discourse -- definitions of classes, relations, functions, and other objects --. This allows researchers to share and reuse information in a specific domain, while retaining the computational benefits of specialized implementations [Gruber 1993]

That is, an ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents. This definition is consistent with the usage of ontology as set-of-concept-definitions, but more general. And it is certainly a different sense of the word than its use in philosophy.

What is important is what an ontology is for. Ontologies are conceived for the purpose of enabling knowledge sharing and reuse. In that context, an ontology is a specification used for making ontological commitments. Although this is not the only way to specify a conceptualization, it has a few appropriate properties for knowledge sharing. Practically, an ontological commitment is an agreement to use a vocabulary (i.e., ask queries and make assertions) in a way that is consistent (but not complete) with respect to the theory specified by an ontology. We design ontologies so we can share knowledge with and among agents (agents can be human as well as automatic machines, like computers).

The term is borrowed from the field of philosophy, where an ontology is a systematic account of existence. For an information system, what "exists" is that which can be represented. When the knowledge of a domain is represented in a declarative formalism, the set of objects that can be represented is called the universe of discourse. This set of objects, and the describable relationships among them, are reflected in the representational vocabulary with which a knowledge-based program represents knowledge. [Gruber 1993]

Pragmatically, a common ontology defines the vocabulary with which **queries and assertions are exchanged among agents**. Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner. The agents sharing a vocabulary need not share a knowledge base; each knows things the other does not, and an agent that commits to an ontology is not required to answer all queries that can be formulated in the shared vocabulary.

5.2.2 A METHOD TO DEFINE ONTOLOGIES

Several methods exist to gain insight into a particular subject and to define an ontology about a specific domain space (domain-specific ontology). In recent years, the concept of ontology has reached the distributed computer domain, in particular in the so-called Semantic World-Wide Web (Tim Berners-Lee has described the semantic web as a component of "Web 3.0") area, therefore emphasizing an approach which targets primarily to the information sharing between automatic agents (computers). [Berners-Lee 2001]

The most widespread methodology currently used to describe ontologies, which is particularly useful for an automatic treatment of the information, is actually that for the Semantic Web, namely the DARPA/DAML specifications. (The Defense Advanced Research Projects Agency (DARPA), in conjunction with the W3C, is developing DARPA Agent Markup Language (DAML) by extending

RDF with more expressive constructs aimed at facilitating agent interaction on the Web [Hendler 2000]).

In this work, we loosely follow DARPA specifications and methodology in defining an ontology for cyber crime and cyber security.

The DARPA/DAML approach

An in-depth guide and tutorial to develop ontologies based on the DARPA methodology can be found at Stanford University Web page [Stanford]: .

Essentially the methodology is iterative, and here we summarize the basic concepts and work flow.

The main activities in defining an ontology are:

- defining the **domain** the ontology will cover
- defining **classes** (concepts) in the ontology
- arranging the classes in a taxonomic (subclass–superclass) hierarchy
- defining **slots** (properties) and describing allowed values for these slots
- filling-in the values for slots for instances.

The important concepts in the method are:

Classes: these are the concepts identified for the domain space. The granularity of class definition can be course or finer, as a matter of choice, and depends on the level of abstraction and insight an ontology will represent.

Taxonomic hierarchy: the classes are translated in a taxonomy, and the taxonomy is represented in a hierarchical (subclass-superclass) tree-like structure.

Slots: slots are the properties of the classes previously defined. For instance, if a class was defined to be *Air*, a slot could be *AirTemperature* or *AirHumidity*.

Slot value types and cardinality: slot must have value type, like numeric (integer, float,...), string, enumerated, instance-type, as well as cardinality (the range of value a slot can cover). For example *AirTemperature* has numeric value-type, which cardinality that could be equivalent to the real interval $[-40^{\circ}\text{C}, +60^{\circ}\text{C}]$.

Naming convention and other details are defined in the DARPA specifications. As mentioned before, more explanations can be found at Stanford Web Site.


(Remark: Examples of already defined ontologies conforming to DARPA/DAML specifications can be found at the link <http://www.daml.org/ontologies/uri.html>).

5.2.3 LIST OF ALL POSSIBLE ASSETS AND ASPECTS RELATED TO CYBER CRIME

We turn now to identifying the domain space of cyber crime / cyber security.

From Table 1 of Section 4.1, it can be deduced the following concepts about cyber crime.

(Please note: the following lists and subsequent related sections and subsections are for illustrative purposes only; they are not exhaustive and may be adapted and extended at any time):

	Roadmapping methodologies and guidelines for information collection and assessment
	Funded by the European Commission under the Seventh Framework Programme
	Page 49 of 65

Types of attack:

<ul style="list-style-type: none"> spam 	the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.
<ul style="list-style-type: none"> phishing scheme 	the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication
<ul style="list-style-type: none"> spyware 	is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
<ul style="list-style-type: none"> malware 	Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems
<ul style="list-style-type: none"> exploit 	is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized)
<ul style="list-style-type: none"> botnet 	a botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.
<ul style="list-style-type: none"> backdoor 	a backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
<ul style="list-style-type: none"> ransomware 	is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed
<ul style="list-style-type: none"> social engineering 	in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information
<ul style="list-style-type: none"> clumsy behaviour 	is the conception that some people might have predisposition, or that they might be more likely to suffer accidents, such as car crashes and industrial injuries, than other people
<ul style="list-style-type: none"> misinformation 	is false or inaccurate information that is spread unintentionally
<ul style="list-style-type: none"> physical damaging 	-
<ul style="list-style-type: none"> insider attacks 	Attacks perpetrated internally. Given the natural view of a conventional firewall on the networks topology as consisting of an inside and outside, problems can arise, once one or more members of the policy network domain have been compromised by internal staff.



The fundamental motivations of cyber attacks:

• financial drivers	Monetary gain, financial advantages, insider information
• governmental reasons	Sabotage of critical infrastructures, ideological and political activism, terrorism
• vengeance	
• reputation	
• stalking	
• verification of systems to improve them	
• unintentional	Unintentional damaging

Possible attacker categories:

• criminal groups, organized crime
• espionage groups
• insider
• phisher
• spammer
• malware attacker
• terrorist
• activist
• military
• intelligence agency

Targets:

• industry
• finance
• government
• military
• private

Means of cyber crime:

• social network
• e-mail
• networks (Internet)
• smartphone
• computer
• home automation
• industrial and control system (SCADA/PLC/HMI)
• payment and on-line financial services
• embedded systems
• unmanned vehicles
• technological assets (health/medical, car, consumer electronics)
• critical infrastructure (military facility, nuclear plant, national level infrastructures)
• communication infrastructures



5.2.4 COLLECTION OF ALL CYBER SECURITY ASPECTS

A collection of cyber security concepts can be also deduced from the previous analysis of the cyber crime domain and from further sources of data [Singh 2013] [Homeland 2009] [Mickelberg 2014].

Cyber security technologies:

• Malware analysis
• Sandboxing
• Blacklists / Blocklists / Host files
• Security policies
• Cloud security
• Virtualization security
• VPN security
• Data Loss Prevention (DLP)
• Denial of Service (DoS / DDoS) Protection
• Anti-virus
• Statistical analysis tools
• Early warning systems
• Encryption
• Endpoint security software
• File Integrity Monitoring (FIM)
• Identity management systems
• Intrusion detection/prevention systems (IDS/IPS)
• Mobile device /Application management (MDM/MAM)
• Network behavioural analysis (NBA)
• Network-based security
• Firewall
• Penetration tests
• Risk assessments
• Secure Gateway
• Security data management analysis
• Threat analysis
• Vulnerability management (VM)
• Security Information & Event Management (SIEM)
• Reputation Management
• Signals Intelligence (SIGINT)
• Human intelligence collection (HUMINT)
• Open-source intelligence (OSINT)
• Managed security service provision (MSSP)
• Payment Card Industry Data Security Standards (PCI DSS)
• Threat and digital object classification (YARA, STIX, CyBox, ZeroMq... etc.)

Vulnerability:

• Secure technologies not available or insufficient
• Cyber security training insufficient
• Cyber security awareness insufficient among the employees
• No secure design during software development
• Security management support missing or insufficient



- Poor interoperability between security solutions

Ethical and legal aspects:

The neologism **Cyberethics** refers to the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society (a valuable overview of cyberethics from the point of view of philosophy is given in [Bynum 2011]). Ethical aspects in the cyber security research area is gaining importance, although specialists practitioners and even researchers in the sector still tend to underestimate its importance. Therefore it must be addressed one way or another. Moreover, legal and regulatory implications necessarily have to be taken into account in the course of all cyber security research activities. Moreover a distinction is made between “Legal/regulatory” and “Purely ethical” aspects. A list of the principal cyber security ethical notions has been distilled from [Brey 2007], [Burstein 2008], [IEEE 2014], [Johnson 2011], [Kenneally 2010], [Schrittwieser 2013], [SecureWorks 2002], and reported in the following table:

Type	Concept	Description
<i>Legal / regulatory</i>		
	• privacy rights	
	• computer abuse	
	• contract law	
	• tort	A tort , in common law jurisdictions, is a civil wrong that unfairly causes someone else to suffer loss or harm resulting in legal liability for the person who commits the tortious act, called a <i>tortfeasor</i>
	• fraud	
	• child pornography	
	• causing injury or death	
	• property rights	
	• intellectual property rights	
	• other civil rights	
	• safety	
	• environmental damaging	
<i>Purely ethical</i>		
	• data confidentiality	
	• data integrity	
	• data availability	
	• data disclosing	
	• data origin	
	• weakening of defences due to data mining activities	
	• discrimination concerns	
	• reputation harm	



	• informed consent	
	• professional code (deontology)	
	• abuse of biometric technics	
	• surveillance harms	
	• altering countersurveillance	
	• persons well-being	

5.2.5 STAKEHOLDERS OF CYBER SECURITY

From the above analysis, the key stakeholders of cyber security turn out to be identified as:

• Owners of assets and operators
• Software vendors and integrators
• Government and state-owned agencies
• Industry organizations
• R&D organizations and laboratories
• Education institutions (universities, high-schools, ...)

5.2.6 CLASSIFICATION OF THE TARGETS

Targets of cyber crime can further be classified in relationship with cyber security:

- **Direct targets:** cyber security is the crime and gives direct results
- **Indirect targets:** cyber security used as a way to prepare and carry out a crime

[Consoli 2014]

5.2.7 DESCRIPTION OF THE ONTOLOGY

An ontology categorizes the problem space and defines a taxonomy for researchers who need to share information in the domain. It includes definitions of basic concepts in the domain and relations among them.


As described in Section 4.2.2 to create the Ontology for cyber security, the DARPA/DAML specifications have been followed.

5.2.8 AN ONTOLOGY FOR CYBER SECURITY

The ontology defined for the cyber crime / cyber security domain space has been built following those additional criteria:

- Top-level classes are directly defined based on the two main themes of the field: cyber crime and cyber security
- Main classes and slots' values have been defined strictly following the classification proposed during the analysis stage of sections 5.2.2-5.2.4
- To define slots, values have been grouped together following the semantic of the parent class: e.g., slots relating to the class *AttackTarget* where created by grouping values following the meaning of the concept "Target" (i.e., "by target groups")

In the following part of this subsection, the ontology for the identified cyber crime / cyber security domain space is schematically presented the

	Roadmapping methodologies and guidelines for information collection and assessment
	Funded by the European Commission under the Seventh Framework Programme
	Page 54 of 65

DOMAIN OF THE ONTOLOGY: Cyber crime / Cyber terrorism / Cyber security

CLASSES

CyberCrime
CyberCrime Attacker
CyberCrime AttackMean
CyberCrime AttackMotivation
CyberCrime AttackTarget
CyberCrime AttackType
CyberTerrorism
CyberTerrorism Attacker
CyberTerrorism AttackMean
CyberTerrorism AttackMotivation
CyberTerrorism AttackTarget
CyberSecurity
CyberSecurity.Ethics
CyberSecurity.Stakeholder
CyberSecurity.TechnologicalTechnique
CyberSecurity.NonTechnologicalTechnique
CyberSecurity.Vulnerability

TAXONOMY (HIERARCHY)

CyberSpace

	CyberCrime
	Attack
	Attacker
	AttackMean
	AttackMotivation
	AttackTarget
	AttackType
	CyberTerrorism
	Attack
	Attacker
	AttackMean
	AttackMotivation
	AttackTarget
	AttackType
	CyberSecurity
	Ethics
	Stakeholder
	TechnologicalTechnique
	NonTechnologicalTechnique
	Vulnerability

PROPERTIES

Class	Slot	Values(*)
CyberCrime.Attacker	criminal_group	thief, espionage
	activist_group	activist, other
	professional	insider, penetration_tester, spammer
	individual	phisher, spammer,



Roadmapping methodologies and guidelines for information collection and assessment

Funded by the European Commission under the Seventh Framework Programme

		malware_attacker
CyberCrime.AttackMean	network_infrastructure	email, ip_device, router, firewall,...
	social_network	facebook, twitter,...
	computer	server, desktop, laptop, notebook
	mobile	smartphone, tablet
	facility	control_system, financial_service
	infrastructure	communication_infrastructure, home_automation critical_infrastructure
	technological_asset	embedded_system, unmanned_vehicle
CyberCrime.AttackMotivation	security_reduction	reputation, system_verification
	protection_reduction	governmental, financial, industrial
	safety_reduction	vengeance, stalking, unintentional
CyberCrime.AttackType	viral	malware, spyware, backdoor, botnet, exploit
	psychological	spam, social_engineering, ransomware, phishing_scheme
	physical	clumsy_behaviour, physically_damaging
CyberCrime.AttackTarget	direct	industry, finance, government, military, civil, private
	indirect	industry, finance, government, military, civil, private(**)
CyberTerrorism.Attacker	organized_group	thief, espionage
	activist_group	terrorist, activist
	professional	insider, penetration_tester,
	individual	phisher, malware_attacker
CyberTerrorism.AttackMean	network_infrastructure	email, ip_device, router, firewall,...
	social_network	facebook, twitter,...
	computer	server, desktop, laptop, notebook
	mobile	smartphone, tablet
	facility	control_system, financial_service
	infrastructure	communication_infrastructure, home_automation critical_infrastructure
	technological_asset	embedded_system, unmanned_vehicle
CyberTerrorism.AttackMotivation	security_reduction	reputation, system_verification
	protection_reduction	governmental, financial, industrial
	safety_reduction	vengeance, stalking, unintentional
CyberTerrorism.AttackType	viral	malware, spyware, backdoor, botnet, exploit
	psychological	spam, social_engineering, ransomware, phishing_scheme
	physical	clumsy_behaviour, physically_damaging
CyberTerrorism.AttackTarget	direct	industry, finance, government, military, civil, private



	indirect	industry, finance, government, military, civil, private(**)
CyberSecurity.Ethics	legal	privacy, computer_abuse, contract_law, tort, injury_or_death, fraud, child_pornography, property_rights, intellectual_property_rights, other_civil_rights, safety, environmental_damaging
	purely_ethical	data_confidentiality, data_integrity, data_availability, data_disclosing, data_origin, defences_weakening_caused_by_data_mining, discrimination_concerns, reputation_harm, informed_consent, professional_code, biometric_techniques_abuse, surveillance_harm, altering_countersurveillance, persons_well_being
CyberSecurity.Stakeholder	professional_individual	operator, professor, teacher
	professional_group	vendors_and_integrator, industry_organization
	institution	government_agency, research_and_development
CyberSecurity.TechnologicalTechnique	management	identity_management_systems, vulnerability_management, mobile_device_management
	analytical	malware_analysis, statistical_analysis, network_behavioural_analysis, penetration_test, security_data_management_analysis
	infrastructural	network_based, firewall, secure_gateway, blacklist, security_policies, endpoint_security_software, file_integrity_monitoring, physical_security, smartcard
	distributed	virtualization_security, vpn_security, cloud_security
	preventive	risk_assessment, password_change, password_complexity, data_loss_prevention



		evention, early_warning, sandbox, encryption, intrusion_prevention_system
	protective	dos_protection, antivirus, antispam, antispysware, intrusion_detection_system, biometrics
CyberSecurity.NonTechnol ogicalTechnique	regulatory	security_policy, usage_regulation,
	educational	behavioural_rule, awareness_measure
	analytical	social_engineering_assessment, other
CyberSecurity.Vulnerabilit y	structural	technology_insufficient, poor_interoperability, no_secure_design, human_resource_lack, committed_management_lack, planning_lack
	human (or contingent)	training_insufficient, awareness_insufficient, management_support_insufficient

(*) all value types turned out to be of the *enumerated* type

(**) notice also that a few slots have equal value denominations, albeit keeping different semantic.

Example of usage of the Ontology

As an example of using the conceptualization expressed by the proposed taxonomy, one can classify for instance the concept expressed in the statement “The antivirus software in the pc is no more maintained, therefore being out of date” in *CyberSecurity.Vulnerability.structural* with value *technology_insufficient*.

5.2.9 STANDARD LANGUAGES FOR THE ONTOLOGY

The Web Ontology Language (OWL) is a family of knowledge representation languages or ontology languages for authoring ontologies or knowledge bases. The languages are characterized by formal semantics and RDF/XML-based serializations for the Semantic Web. OWL is endorsed by the World Wide Web Consortium (W3C) and has attracted academic, medical and commercial interest. It is highly recommended to follow OWL specifications for the present work.

(see <http://www.w3.org/2001/sw/wiki/OWL>)

5.3 DATA COLLECTION METHODOLOGY

In this section, a methodology for information gathering from sources is presented.

The data collection methodology is directly based on the pattern followed in conceptualizing the problem space and in defining the ontology for cyber crime / cyber security.

5.3.1 SOURCES OF INFORMATION AND RELATED CLASSIFICATION

Sources of information can be deduced and grouped directly from the ontology of section 5.2, in particular from the classes *AttackTarget*, *AttackMotivation* and, most important, from the *CyberSecurityStakeholders* class.

The following list presents the results:

• Managers and technical employees in system and software engineer organizations
• Managers and technical employees in integration engineer organizations
• Professors and researchers in educational institutions (universities, colleges)
• Managers and coordinators in public organizations
• Managers and coordinators in private organizations (industry, services, finance, banks, health and medical)
• Employees in public organizations
• Employees in private organizations (industry, finance, banks, health and medical)
• Data collected in automatic or semi-automatic way from specialized online services.
• Literature on cyber crime / cyber security
• Data gathered from institutions and other organizations.

5.3.2 METHODOLOGY TO DEFINE GROUPS OF PEOPLE TO BE INTERVIEWED

This section defines criteria to select *Focus groups* of people to be interviewed and presents the outcome of the grouping.

In view of the main goal of the CyberRoad project – define a roadmap for research activities in the cyber security field - the most natural criterion, and the one chosen in this work, consists in organizing the interviewees following a **scale of technical competences/expertise** in relation to the computer science/cyber security field. In this way, one can easily adapt the kinds of questions to the skill level of the interviewed people. The Table 2 shows the grouping of potential interviewees, based on four levels of expertise in the cyber security domain.

Table 2: Level of expertise of interviewees

Denomination of the group	Level of expertise/skill	Group of interviewed persons	Mainly employed in
VHLE	Very High	Professor and researchers, technical staff in the cyber security field.	Public, private sector
HLE	High	Technical employees in computer engineering (not in cyber security field).	Public, private sector
MLE	Medium	Managers, supervisors coordinators.	Private, public sector
LLE	Low	People expert in other sectors, usually with an academic degree	Private, public sector
VLLE	Very-low	General employees, with scarce or no academic preparation	Private, public sector



5.3.3 METHODOLOGY OF INTERVIEWING

Basing on the grouping outcome of section 5.3.2, one can define the methodology of conducting the interviews. The methodologies are therefore illustrated in Table 3.

Table 3: Interviewing methodologies

Group of interviewees	Method of interviewing	Typology of questions
VHLE	A highly-technical cyber-security sector-specific language can be used.	Questions can be in-depth and very specific to the particular subfield and skill of the interviewee.
HLE	A technical language in general computer science and engineering can be utilized, not excessively technical as far as the cyber security arguments are concerned.	Questions about cyber security must be kept at a quite general, though still technical, level.
MLE	Possibly a technical language in general computer science and engineering should be utilized. Nevertheless more emphasis has to be put on organizational and business aspects.	Questions about cyber security must be kept at a general level, emphasizing at the same time the business aspects.
LLE	Poor technical language of the cyber security domain can be used.	Questions must be of general concern and should be put in a form avoiding technical terms specific of cyber security domain, but can use some concepts of general computer science
VLLE	Poor or no technical language can be used.	Questions must possibly avoid all kinds of technical terminology. Concepts should be “translated” in a quite colloquial language

5.3.4 METRICS FOR RANKING OF THE SOURCES

Sources, independently from their nature (human, material, ...) can be classified in a similar manner as the groups of interviewees, in other words considering the **technical level** (in the cyber security domain). The values of the metric range from 1 (the lowest technical level) to 5 (the highest technical level). Table 4 below reports the ranking of these categories.

Table 4: Ranking of sources

Rank	Technical level	Sources	People mainly concerned
5	Very High	<ul style="list-style-type: none"> Literature on cyber crime/cyber security Academics opinion 	Professors, researchers, computer engineers involved in cyber security domain
4	High	<ul style="list-style-type: none"> Data collected from the Internet Computer science engineers 	Technical staff, practitioners



3	Medium	<ul style="list-style-type: none"> Literature on general computer science. 	Computer Engineers (in general)
2	Low	<ul style="list-style-type: none"> Far cyber security-related fields Experts in other fields 	People with an academic degree, but not in computer science related fields
1	Very Low	<ul style="list-style-type: none"> Common people opinion, with only practical experience with IT devices, journalists. 	People with no academic degree in technical/scientific disciplines

5.3.5 TEMPLATE OF THE QUESTIONNAIRES

The information and insights reached in the previous sections of this document, can now be translated into the design of a common template for questionnaires that can be used to conduct interviews and gather data from the typologies of potential stakeholders.

The discrimination between the above-identified groups of interviewees (VHLE, HLE, MLE, LLE and VLLE) is carried out in the guidelines for the information reporting and assessment (presented in section 5.4 below).

The resulting template for interviewing questionnaires is given **in annex** to this document.

5.4 GUIDELINES TO ASSESS AND REPORT INFORMATION

A questionnaire template common to all interview typologies has been defined in the previous section. Here we present guidelines to select queries and assess and report the gathered information

1. Identify a proper sample of potential interviewees, taking care to obtain similar amounts between possible subsets of stakeholders – refer to section 5.3.2.
2. Identify the group which the interviewee is belonging to. Possible groups have been identified based on the skill/expertise level in the field: VHLE (very high level of expertise), HLE (high level of expertise), MLE (medium level of expertise), LLE (low level of expertise) and VLLE (very low level of expertise) – refer to section 5.3.2.
3. Starting from the identified expertise group, select the appropriate subset of queries in the questionnaire and the appropriate language to conduct the interview – refer to section 5.3.3
4. Having collected the filled in questionnaires, group the gathered information on the basis of the metric defined to rank the sources – refer to section 5.3.4

5.5 FORM TO PRESENT THE RESULTS

A definitive form to present data and results will be decided once the project starts to produce outcomes.

6 CONCLUSIONS

The deliverable D2.1 is the first, in chronological order, of the CyberRoad project. It has therefore four basic purposes:

- the first one is to propose a definition and characterization of the problem space;
- the second purpose is to present a survey on the available methodologies suitable to define a roadmap to conduct cyber security researches;
- the third purpose is to define a taxonomy (an ontology) covering the cyber crime / cyber security domain space, useful to share information between stakeholders (researchers);
- the fourth purpose is to design guidelines for collect and assess information from potential stakeholders of cyber security-related technologies. The information collected represents a base of more in-depth discussion during the continuation of the project, and will be used further to define the methodology for risk assessment ranking (T2.2).

7 REFERENCES AND BIBLIOGRAPHY

- [Asgher 2013] Asgher, U., Analysis of Increasing Malwares and Cyber Crimes Using Economic Approach, The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, 2013.
- [Ayofe 2009] Ayofe, A. N., Oluwaseyifunmitan, O., Towards Ameliorating Cybercrime and Cybersecurity, International Journal of Computer Science and Information Security, Vol. 3, No. 1
- [Austra 2013] National Plan to Combat Cybercrime, Australian Government, 2013
- [Beeton 2007] Beeton, D.A. Exploratory roadmapping for sector foresight. PhD thesis, University of Cambridge, 2007
- [Beeton 2008] Beeton, D.A., Phaal, R., Probert, D.R. Exploratory roadmapping for foresight. International Journal of Technology Intelligence and Planning 4(4), 398-412, 2008
- [Beeton 2013] Beeton, D., Phaal, R., Probert, D. Exploratory Roadmapping: Capturing, Structuring and Presenting Innovation Insights. In: [Möhrle 2013], 225-240, 2013
- [Benenson 2011] Benenson, Z., Exploring the Landscape of Cybercrime, Friedrich-Alexander-University Erlangen-Nuremberg, Germany, 2011.



- [Berners-Lee 2001] Berners-Lee, T., "The Semantic Web". Scientific American, 2001
- [Burstein 2008] Burstein, A. J., Conducting Cybersecurity Research Legally and Ethically, University of California, Berkeley (School of Law), 2008
- [Brey 2007] Brey, P., "Ethical Aspects of Information Security and Privacy", in: Security, Privacy, and Trust in Modern Data Management, M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36, 2007
- [Bynum 2011] Bynum, Terrell, "Computer and Information Ethics", *The Stanford Encyclopedia of Philosophy* (Spring 2011 Edition), Edward N. Zalta (ed.), (<http://plato.stanford.edu/archives/spr2011/entries/ethics-computer>)
- [Carvalho 2013] Carvalho, M.M., Fleury, A., Lopes, A.P. An overview of the literature on technology roadmapping (TRM): Contributions and trends. *Technological Forecasting & Social Change* 80, 1418-1437, 2013
- [Choi 2013] Choi, S., Kim, H., Yoon, J., Kim, K., Lee, J.Y. An SAO-based text-mining approach for technology roadmapping using patent information. *R&D Management* 43(1), 52-74, 2013
- [Ciardhuáin 2004] Ciardhuáin, S. Ó., "An Extended Model of Cybercrime investigations," 2004.
- [Codagnone 2007] Codagnone C., Wimmer, M.A. (Eds.): Roadmapping eGovernment Research - Visions and Measures towards Innovative Governments in 2020. Results from the EC-funded Project eGovRTD2020 IST-2004-027139, 2007, <http://www.egovrtd2020.org>
- [Consoli 2014] Consoli A., Master in ICT Systems and Security, SUPSI, Switzerland, 2014
- [Correa 2013] Correa, D., Sureka, A., Solutions to Detect and Analyze Online Radicalization : A Survey, Indraprastha Institute of Information Technology - Delhi, India, 2013
- [CSEC 2013] Communications Security Establishment Canada (CSEC), Cyber Security Research and Experimental Development Program, 2013.
- [Daim 2014] Daim, T.U., Pizarro, M., Talla, R. (Eds.): Planning and Roadmapping Technological Innovations - Cases and Tools. Springer, 2014. ISBN 978-3-319-02972-6
- [DARPA/DAML] DARPA/DAML, List of Ontologies by URI, <http://www.daml.org/ontologies/uri.html>
- [Da Costa 2005] Da Costa, O., Boden, M., Friedewald, M. Science and Technology Roadmapping for Policy Intelligence. Lessons for Future Projects. In: Proc. 2nd Prague Workshop On Futures Studies Methodology, 146-161, 2005
- [Enisa 2013] Enisa, Roadmap for European Cyber Security Month, ECSM final report, 2013
- [Geschka 2013] Geschka, H., Hahnenwald, H. Scenario-Based Exploratory Technology Roadmaps - A Method for the Exploration of Technical Trends. In: [Möhrle 2013], 123-136, 2013
- [Gruber 1993] Gruber, T. R., A Translation Approach to Portable Ontology Specifications, Knowledge System Laboratory, Stanford University, 1993.
- [Gupta 2013] Gupta, H., Meena, M., Digital Crime Investigation using Various Logs and Fuzzy Rules: A Review, Patel Institute of Technology, Bhopal, India, 2013
- [Hendler 2000] Hendler, J., McGuinness, D.L., The DARPA Agent Markup Language, IEEE Intelligent Systems 16(6), 2000



- [Homeland 2009] A roadmap for cybersecurity research, U.S. Department of Homeland Security, 2009.
- [ICSJWG 2011] The ICSJWG Roadmap Working Group, Cross-Sector Roadmap for Cybersecurity of Control Systems, 2011.
- [IEA 2010] Energy Technology Roadmaps; a guide to development and implementation, International Energy Agency, Paris, 2010
- [IEEE 2014] IEEE, IEEE Code of Ethics
(<http://www.ieee.org/about/corporate/governance/p7-8.html>)
- [Industry Canada] Industry Canada (Department of the Canadian Government)
<http://www.ic.gc.ca/eic/site/trm-crt.nsf/eng/Home>
"Technology Roadmapping in Canada: A Development Guide",
[https://www.ic.gc.ca/eic/site/trm-crt.nsf/vwapj/development-developpement_eng.pdf/\\$file/development-developpement_eng.pdf](https://www.ic.gc.ca/eic/site/trm-crt.nsf/vwapj/development-developpement_eng.pdf/$file/development-developpement_eng.pdf)
"Evaluating Technology Roadmaps: A Framework for Monitoring and Measuring Results",
[https://www.ic.gc.ca/eic/site/trm-crt.nsf/vwapj/evaluation_eng.pdf/\\$file/evaluation_eng.pdf](https://www.ic.gc.ca/eic/site/trm-crt.nsf/vwapj/evaluation_eng.pdf/$file/evaluation_eng.pdf)
- [James 2013] James, J. I., Jang, Y. J., An Assessment Model for Cybercrime Investigation Capacity, Digital Forensic Investigation Research Group, University College Dublin, 2013
- [Jeffrey 2013] Jeffrey, H., Sedgwick, J., Robinson, C. Technology roadmaps: An evaluation of their success in the renewable energy sector. Technological Forecasting & Social Change 80, 1015-1027, 2013
- [Johnson 2011] Johnson, M. L., Bellovin, S. M., Keromytis, A. D., Computer Security Research with Human Subjects: Risks, Benefits and Informed Consent, Columbia University, 2011
- [Kanama 2013] Kanama, D. Moehrle, M. G. Development of Technology Foresight: Integration of Technology Roadmapping and the Delphi Method. In: [Möhrle 2013], 151-171, 2013
- [Kanich 2011] Kanich, U. C., No Plan Survives Contact: Experience with Cybercrime Measurement, Department of Computer Science and Engineering, University of California, San Diego, 2011.
- [Kenneally 2010] Kenneally, E., Bailey, M., Maughan, D., A Framework for Understanding and Applying Ethical Principles in Network and Security Research, 2010
- [Kerr 2008] Kerr, C., Phaal, R., Probert, D. A strategic capabilities-based representation of the future British armed forces. International Journal of Intelligent Defence Support Systems 1(1), 27-42, 2008
- [Kerr 2013] Kerr, C., Phaal, R., Probert, D. Roadmapping as a Responsive Mode to Government Policy: A Goal-Orientated Approach to Realising a Vision. In: [Möhrle 2013], 67-87, 2013
- [Kostoff 2001] Kostoff, R.N., Schaller, R.R. Science and Technology Roadmaps. IEEE Transactions on Engineering Management 48(2), 132-143, 2001
- [Lizaso 2004] Lizaso, F., Reger, G. Scenario-based roadmapping - a conceptual view. EU-US Scientific Seminar on New Technology Foresight, Forecasting & Assessment Methods, Seville, Spain, 2004
- [Londo 2013] Londo, H.M., More, E., Phaal, R., Wütenberger, L., Cameron, L. Background paper on technology roadmaps, Report for United Nations Framework Convention on Climate Change (UNFCCC), 2013
- [Mickelberg 2014] Mickelberg, K., US cybercrime: Rising risks, reduced readiness, PricewaterhouseCoopers LLP, 2014.
- [Möhrle 2013] Möhrle, M.G., Isenmann, R., Phaal, R. (Eds.): Technology roadmapping for



strategy and innovation: charting the route to success. Springer, 2013. ISBN 978-3642339226

- [NIST 2014] Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2014.
- [Phaal 2001] Phaal, R., Farrukh, C.J.P., Probert, D.R. T-Plan: the fast-start to technology roadmapping planning your route to success. Institute for Manufacturing, University of Cambridge, 2001
- [Phaal 2007] Phaal, R., Farrukh, C.J.P., Probert, D.R. Strategic roadmapping: a workshop-based approach for identifying and exploring innovation issues and opportunities. Engineering Management Journal 19(1), 16-24, 2007
- [Phaal 2013a] Phaal, R., Farrukh, C., Probert, D. Fast-Start Roadmapping Workshop Approaches. In: [Möhrle 2013], 91-106, 2013
- [PWC 2014] PricewaterhouseCoopers LLP, US cybercrime: Rising risks, reduced readiness, 2014
- [Raggad 2007] Raggad, B. G., Cyberspace security: How to develop a security strategy, Pace University, Pleasantville, N.Y., 2007.
- [Schrittwieser 2013] Schrittwieser, S., Mulazzani, M., Weippl, E., Ethics in Security Research. Which Lines Should Not Be Crossed?, Vienna University of Technology, 2013
- [SecureWorks 2002] Dell SecureWorks, Crossing the Line: Ethics for the Security Professional, 2002
- [Singh 2013] Singh, N., Rani, S. The Roadmap for Cyber Crime Investigation, International Journal of Electronics and Computer Science Engineering, Volume 2, Number 2 2013.
- [Stanford] Noy, N. F., McGuinness, M. L., Ontology Development 101: A Guide to Creating Your First Ontology
http://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html, Stanford University, Stanford, CA

- End of Document -





Funded by the European Commission

Seventh Framework Programme



CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Questionnaire for interview (Annex to deliverable D2.1)

Version: 0.7



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 17

Revision history

Version	Object	Date	Author(s)
0.1	Creation	26/06/2014	SUPSI
0.2	...	29/08/2014	UNICA
0.3	...	30/08/2014	SUPSI
0.3	...	01/09/2014	SUPSI
0.4	...	02/09/2014	SUPSI
0.5	...	02/09/2014	ALL
0.6	...	11/09/2014	SUPSI
0.7	final version	12/09/2014	SUPSI



This document is a major outcome of the task T2.1. of the CyberRoad project. It represents a template for the questionnaires suitable for conducting interviews to stakeholders.

Stakeholders have been classified and groups have been defined in the deliverable D2.1 of the CyberRoad project. The criteria for classification and the rationale for the content of this template are given in the deliverable.

This questionnaire template is attached in Annex to the deliverables D2.1 “Roadmapping methodologies and guidelines for information collection and assessment”.

Remark: The present version of the questionnaire should be understood as a template, which will be improved in the course of the project to reach the final form.

Organization/company name (optional): _____

Organization type (Public/Private/R&D/Health/Governmental): _____

Field of operation of the organization: _____

Size of the company: _____

- ☐ Medium-sized (<250 persons, <= €50 million annual turnover)
- ☐ Small (<50 persons, <= €50 million annual turnover)
- ☐ Micro (<10 persons, <= €2 million annual turnover)

Country: _____

Function/Position inside the organization: _____

- ☐ CISO
- ☐ COO
- ☐ CEO
- ☐ Security manager
- ☐ Security assistant
- ☐ IT professional (not specifically focused on cyber security)
- ☐ Legal body/professional
- ☐ Other: _____

Definitions

(Remark : the definitions provided below are for guidance only and will be made in full form in the final version of the questionnaire)

Cyber security

The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Cyber attacks

A cyber attack is an intentional breach of confidentiality, integrity, availability, authenticity and non-repudiation of an information system.

Cyber crime

Cyber crime encompasses two forms of criminal activities: the use of computer system to enable traditional form of criminal activity (e.g., child pornography, money laundering); and the use of a computer system to launch a cyber attack (as understood by the aforementioned definition).

Cyber terrorism

The use of a cyber attack breaching components of information security, instigated in order to achieve political motives largely of a subversive nature, and resulting in either physical destruction or loss of life.

3 QUESTIONS RELATED TO CYBER CRIME ASPECTS

3.1 WHAT ARE THE MOST PROBABLE TYPES OF CYBER CRIME ACTIVITIES?

(RANKING: 1 FOR THE LESS LIKELY, 6 FOR THE MOST LIKELY)

Explanation/justification of the question

Type of cyber attack	1	2	3	4	5	6
Spams	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phishing activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spywares	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Malwares	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Exploitations (DoS, DDoS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Botnet activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backdoors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social engineering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clumsy behavior	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical damaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate)						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.2 WHAT ARE THE MOST PROBABLE TYPES OF CYBER TERRORISM ACTIVITIES?

(RANKING: 1 FOR THE LESS LIKELY, 6 FOR THE MOST LIKELY)

Explanation/justification of the question

Type of cyber attack	1	2	3	4	5	6
Spams	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phishing activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spywares	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Malwares	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Exploitations (DoS, DDoS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Botnet activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backdoors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social engineering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clumsy behavior	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical damaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate)						



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.3 WHICH ARE THE MOST LIKELY MOTIVATIONS BEHIND CYBER ATTACKS ORIGINATED BY CYBER CRIME ?
(RANKING: 1 FOR THE LESS LIKELY, 6 FOR THE MOST LIKELY)

Explanation/justification of the question

Motivation of cyber attack	1	2	3	4	5	6
Financial	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Governmental reasons	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vengeance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reputation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stalking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verification of systems to improve them	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unintentional reasons (clumsy behavior)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.4 WHICH ARE THE MOST LIKELY MOTIVATIONS BEHIND CYBER ATTACKS ORIGINATED BY CYBER TERRORISM ?
(RANKING: 1 FOR THE LESS LIKELY, 6 FOR THE MOST LIKELY)

Explanation/justification of the question

Motivation of cyber attack	1	2	3	4	5	6
Financial	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Governmental reasons	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vengeance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reputation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stalking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verification of systems to improve them	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unintentional reasons (clumsy behavior)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.5 WHICH ARE THE MOST WIDESPREAD TYPOLOGIES OF CYBER CRIME ATTACKERS?
(RANKING: 1 FOR THE LESS WIDESPREAD, 6 FOR THE MOST WIDESPREAD)

Explanation/justification of the question

Attacker	1	2	3	4	5	6
Criminal group, organized crime	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spionage group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phisher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spammer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spyware/malware attacker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activist	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.6 WHICH ARE THE MOST WIDESPREAD TYPOLOGIES OF CYBER TERRORISM ATTACKERS?
(RANKING: 1 FOR THE LESS WIDESPREAD, 6 FOR THE MOST WIDESPREAD)

Explanation/justification of the question

Attacker	1	2	3	4	5	6
Organized group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spionage group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phisher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spyware/malware attacker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Terrorist	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activist	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Remarks: _____

3.7 WHICH ARE THE MOST ATTRACTIVE TARGETS OF CYBER CRIME ACTIVITIES?

(RANKING: 1 FOR THE LESS ATTRACTIVE, 6 FOR THE MOST ATTRACTIVE)

Explanation/justification of the question

Target of cyber attacks	1	2	3	4	5	6
Industry organizations and plants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Finance, services and banks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government / national facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Military installations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Civil installations (energy, environment, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Citizens privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.8 WHICH ARE THE MOST ATTRACTIVE TARGETS OF CYBER TERRORISM ACTIVITIES?

(RANKING: 1 FOR THE LESS ATTRACTIVE, 6 FOR THE MOST ATTRACTIVE)

Explanation/justification of the question

Target of cyber attacks	1	2	3	4	5	6
Industry organizations and plants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Finance, services and banks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government / national facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Military installations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Civil installations (energy, environment, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Citizens privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Remarks: _____

3.9 WHICH ARE THE MOST KNOWN MEANS OF CYBER CRIME ACTIVITIES?

(RANKING: 1 FOR THE LESS KNOWN MEAN, 6 FOR THE MOST KNOWN MEAN)

Explanation/justification of the question

Mean of cyber attacks	1	2	3	4	5	6
Social networks (Facebook, Twitter, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Networks and network infrastructures (IP devices, routers, firewalls, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart phones / Tablets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Computers (Desktop, Notebook, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Servers and machines always online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Home automation infrastructures and devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Industrial and control systems (SCADA/PLC/HMI)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Automatic payment and on-line financial services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Embedded systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unmanned vehicles (drones, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Technological assets (health/medical devices, cars, consumer electronics)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Critical infrastructures (military facilities, nuclear plant, national level infrastructures)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication infrastructures (telephone network, TV cable network, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

3.10 WHICH ARE THE MOST KNOWN MEANS OF CYBER TERRORISM ACTIVITIES?

(RANKING: 1 FOR THE LESS KNOWN MEAN, 6 FOR THE MOST KNOWN MEAN)

Explanation/justification of the question

Mean of cyber attacks	1	2	3	4	5	6
Social networks (Facebook, Twitter, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Networks and network infrastructures (IP devices, routers, firewalls, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart phones / Tablets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

Computers (Desktop, Notebook, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Servers and machines always online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Home automation infrastructures and devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Industrial and control systems (SCADA/PLC/HMI)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Automatic payment and on-line financial services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Embedded systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unmanned vehicles (drones, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Technological assets (health/medical devices, cars, consumer electronics)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Critical infrastructures (military facilities, nuclear plant, national level infrastructures)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication infrastructures (telephone network, TV cable network, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

4 QUESTIONS RELATED TO CYBER SECURITY ASPECTS

4.1 WHAT ARE THE MOST EFFECTIVE TECHNOLOGICAL TECHNIQUES ADOPTED BY CYBER SECURITY TO PROTECT/PREVENT CYBER CRIME / CYBER TERRORISM ATTACKS? (RANKING: 1 FOR THE LESS EFFECTIVE, 6 FOR THE MOST EFFECTIVE)

Explanation/justification of the question

Technological technique of cyber security	1	2	3	4	5	6
Malware analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sandboxing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blacklists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security policies (ACLs, storage quotes, limits on installation capability,...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Periodic password changes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password complexity requirements	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Website content filtering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cloud security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Virtualization security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Loss Prevention (DLP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

Protection against exploitations (DoS / DDoS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Antivirus software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Antispam software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Antispyware software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Statistical analysis tools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Early warning systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Endpoint security software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File Integrity Monitoring (FIM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identity management systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Intrusion detection systems (IDS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Intrusion prevention systems (IPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mobile device /Application management (MDM/MAM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smartcards (card, PCMCIA, USB, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network behavioural analysis (NBA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network-based security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewalling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Penetration tests	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Risk assessments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical security (i.e. a vault, strong room, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Secure gateways	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Biometrics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security data management analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vulnerability management (VM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

4.2 WHAT ARE THE MOST EFFECTIVE NON TECHNOLOGICAL TECHNIQUES ADOPTED BY CYBER SECURITY TO PROTECT/PREVENT CYBER CRIME / CYBER TERRORISM ATTACKS?

(RANKING: 1 FOR THE LESS EFFECTIVE, 6 FOR THE MOST EFFECTIVE)

Explanation/justification of the question

NON technological technique of cyber security	1	2	3	4	5	6
Security policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Usage regulations (of email, of social networks, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

Behavioural rules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Awareness measures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social engineering assessments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

**4.3 WHICH ARE THE CURRENT MOST SERIOUS WEAKNESSES OF CYBER SECURITY PROTECTIONS?
(RANKING: 1 FOR THE LESS SERIOUS, 6 FOR THE MOST SERIOUS)**

Explanation/justification of the question

Cyber security vulnerabilities	1	2	3	4	5	6
Secure technologies not available or insufficient	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
insufficient Cyber security training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cyber security awareness among employees insufficient	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No secure design during software development	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security management support missing or scarce	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor interoperability between security solutions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of human resources in the organization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of committed management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lack of planning / awareness	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

4.4 WHICH ARE THE MOST SENSIBLE ETHICAL ASPECTS IN CYBER SECURITY ACTIVITIES AND DATA PROTECTION?

(RANKING: 1 FOR THE LESS SENSIBLE, 6 FOR THE MOST SENSIBLE)

Explanation/justification of the question

Ethical aspects in cyber security	1	2	3	4	5	6
privacy rights	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
computer abuse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Questionnaire for interview (Annex to deliverable D2.1)

Funded by the European Commission under the Seventh Framework Programme

contract law (e.g. EULAs, clickwrap/shrinkwrap licenses, disclaimer, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
tort	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
causing injury or death	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
fraud	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
child pornography	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
property rights	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
intellectual property rights (copyright,...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
other civil rights	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
safety	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
environmental damaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data confidentiality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data integrity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data availability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data disclosing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
data origin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
weakening of defences due to data mining activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
discrimination concerns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
reputation harm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
informed consent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
professional code (deontology)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
abuse of biometric technics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____



4.5 IMPROVEMENT I: IN YOUR OPINION, WHAT ARE THE CURRENT GENERAL DOMAINS THAT SHOULD BE ENHANCED IN ORDER TO IMPROVE RESILIENCE AGAINST CYBER CRYME?
(RANKING: 1 FOR THE LESS NEEDING OF ENHANCEMENT, 6 FOR THE MOST NEEDING OF ENHANCEMENT)

Explanation/justification of the question

General domains for enhancement	1	2	3	4	5	6
Industry organizations and plants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Finance, services and banks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government / national facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Military installations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Citizens privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

4.6 IMPROVEMENT I: IN YOUR OPINION, WHAT ARE THE CURRENT GENERAL DOMAINS THAT SHOULD BE ENHANCED IN ORDER TO IMPROVE RESILIENCE AGAINST CYBER TERRORISM?
(RANKING: 1 FOR THE LESS NEEDING OF ENHANCEMENT, 6 FOR THE MOST NEEDING OF ENHANCEMENT)

Explanation/justification of the question

General domains for enhancement	1	2	3	4	5	6
Industry organizations and plants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Finance, services and banks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government / national facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Military installations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Citizens privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others (please indicate, if any):						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____



4.7 IMPROVEMENT II: IN YOUR OPINION, WHAT ARE R&D DOMAINS IN WHICH MORE ATTENTION SHOULD BE FOCUSED TO IMPROVE CYBER SECURITY?

(RANKING: 1 FOR THE LESS NEEDING OF ATTENTION, 6 FOR THE MOST NEEDING OF ATTENTION)

Explanation/justification of the question

R&D domains	1	2	3	4	5	6
Theoretical (cryptography, algorithms, ...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forensic activities enhancement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Networks / Internet protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System protection (servers, PCs, peripherals,...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication infrastructures protection/prevention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Critical infrastructures protection/prevention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Political / social interventions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethical domains research	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, basic scholarship (<15)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, higher education	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, low profile workers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, middle management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, top management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Education / Awareness, IT & Security specialists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
...						
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

5 HOW WOULD YOU RATE THE EFFECTIVENESS OF THE FOLLOWING MEASURES IN THE FIGHT AGAINST CYBER CRIME?

(RANKING: 1 LOW EFFECTIVENESS, 6 HIGH EFFECTIVENESS)

Explanation/justification of the question

Measures	1	2	3	4	5	6
Mandatory reporting of incidents ¹	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create a minimum set of criteria to access internet (if a computer is not sufficiently updated, it is out)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Give the user a ranking to authenticate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Further limit user's freedom	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Others (please indicate, if any):</i>						
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: _____

- End of Document -

¹ As suggested by Dan Geer in his recent keynote at Black Hat US 2014
<http://geer.tinho.net/geer.blackhat.6viii14.txt>