



Funded by the European Commission

Seventh Framework Programme



## CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

# D2.2 Risk Assessment Ranking Methodology

Date of deliverable: 31/05/2015

Actual submission date: 27/05/2015

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

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

Version: 1.0

Project funded by the European Commission under the Seventh Framework Programme		
Restriction Level		
PU	Public	X
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)	



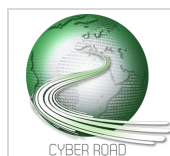
D2.2 Risk Assessment Ranking Methodology

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 57

## Revision history

Version	Object	Date	Author(s)
0.1	Creation	05/09/2014	A. Gralewski, C. Dambra
0.2 - 0.3	Internal versions	30/03/2015	A. Gralewski, C. Dambra
0.4	After comments from partners	15/04/2015	A. Gralewski, C. Dambra
0.5	Final draft after integration of the methodology into the roadmapping approach after discussion with UNICA	28/04/2015	A. Gralewski, C. Dambra
1.0	Final version	22/05/2015	A. Gralewski, C. Dambra



## D2.2

# Risk Assessment Ranking Methodology

### Responsible

A. Gralewski, C. Dambra (PROPRS)

### Contributor(s)

L. Regan (PROPRS)  
F. Roli, G. Giacinto, D. Ariu (UNICA)  
L. Cavallaro (RHUL)  
E. Frumento (CEFRIEL)  
Olga E. Segou (NCSRD)  
J. Armin (CYBERDEFCON)

**Note:** To allow a proper understanding of the ranking process, D2.2 includes in Appendixes the following two documents describing the roadmapping methodology developed in WP2 that will be officially reported in Deliverable D2.3:

- “Creation of Roadmaps based on Scenario Analysis” (Slides)
- “Tutorial on Scenario Analysis & Roadmapping”

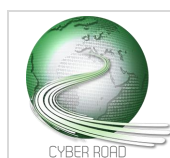
**Summary:** This deliverable describes the risk assessment approach identified to rank research topics in a roadmapping approach. The document starts from the hypothesis that the data collected on these research topics from stakeholders will be subjective, and not of sufficient quality to consider a quantitative approach. Furthermore the lack of sufficiently verified data on frequency-severity of cyberattacks make it difficult to use sophisticated techniques. Therefore the method proposed is based on Boston Square method. The traditional Boston Square method has been tuned to the specificities of the project dealing with cyber-crime and cyber-terrorism research topics and not specific cyber-risks of a given organisation.

**Keywords:** risk assessment, research topics ranking, multi-criteria analysis, Boston Squares



# TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>5</b>
<b>2</b>	<b>GENERAL APPROACH TO RISK ASSESSMENT .....</b>	<b>6</b>
2.1	INTRODUCTION .....	6
2.2	QUALITATIVE RISK ASSESSMENT.....	6
2.3	QUANTITATIVE RISK ASSESSMENT .....	8
2.4	PROPOSED METHODOLOGY .....	8
2.4.1	<i>Risk Criteria .....</i>	<i>9</i>
2.4.2	<i>Definition of System Boundaries.....</i>	<i>9</i>
2.4.3	<i>Data Collection.....</i>	<i>9</i>
2.4.4	<i>Identification of threats/hazards.....</i>	<i>9</i>
2.4.5	<i>Consequence Analysis .....</i>	<i>10</i>
2.4.6	<i>Estimation of Event/threat Frequencies .....</i>	<i>10</i>
2.4.7	<i>Risk Estimates .....</i>	<i>10</i>
2.4.8	<i>Treatment of Uncertainty and Bias.....</i>	<i>11</i>
2.4.9	<i>Risk mitigation/reduction .....</i>	<i>11</i>
2.4.10	<i>Elicitation from experts.....</i>	<i>11</i>
<b>3</b>	<b>APPROACHES TO ELICITATION WITH UNCERTAINTY.....</b>	<b>12</b>
3.1	<i>AGGREGATE OF MULTIPLE UNCERTAIN OUTCOMES.....</i>	<i>13</i>
<b>4</b>	<b>PROPOSED RISK RANKING .....</b>	<b>15</b>
4.1	OVERALL APPROACH FOR RESEARCH RANKING PRIORITISATION.....	15
4.1.1	<i>Define criteria for assessing the priorities for cyber research and its boundary and limits.....</i>	<i>16</i>
4.1.2	<i>Select research topic RT .....</i>	<i>16</i>
4.1.3	<i>Create a list of Cyber Threats.....</i>	<i>16</i>
4.1.4	<i>Create a list of assets affected by each CT.....</i>	<i>17</i>
4.1.5	<i>Calculate all the risks using Boston Square.....</i>	<i>17</i>
4.1.6	<i>Score each Research topic to provide Ranking prioritisation .....</i>	<i>20</i>
<b>5</b>	<b>INTERACTION WITH CYBERROAD WP5 .....</b>	<b>24</b>
<b>6</b>	<b>RISK-BASED RANKING AND THE ROADMAPPING PROCESS.....</b>	<b>26</b>
<b>7</b>	<b>EVOLUTION OF THE RANKING OVER TIME .....</b>	<b>27</b>
	<b>APPENDIX 1 - MCA EXAMPLE.....</b>	<b>28</b>
	<b>APPENDIX 2 - “CREATION OF ROADMAPS BASED ON SCENARIO ANALYSIS” (SLIDES).....</b>	<b>30</b>
	<b>APPENDIX 3 - TUTORIAL ON SCENARIO ANALYSIS AND ROADMAPPING .....</b>	<b>40</b>



# 1 INTRODUCTION

The objective of this report is to develop a methodology for assessing research topics, using risk assessment to provide ranking for priorities in undertaking such research. To this aim the risk assessment undertaken here is only to help to rank the research topic, identified in work-packages from WP3 to WP6, requiring additional studies or new research.

This work is part of Task 2.2 “Methodology for risk assessment ranking” in WP2 “Scientific Coordination” and will serve as input to Task 2.4 “Cybersecurity research roadmap generation” together with the work done in the other technical Work-Packages (see Figure 1):

- WP3 - Social, Economic, Political and Legal Scenario;
- WP4 - Technological Scenario;
- WP5 - Cybercrime
- WP6 - Cyber-terrorism

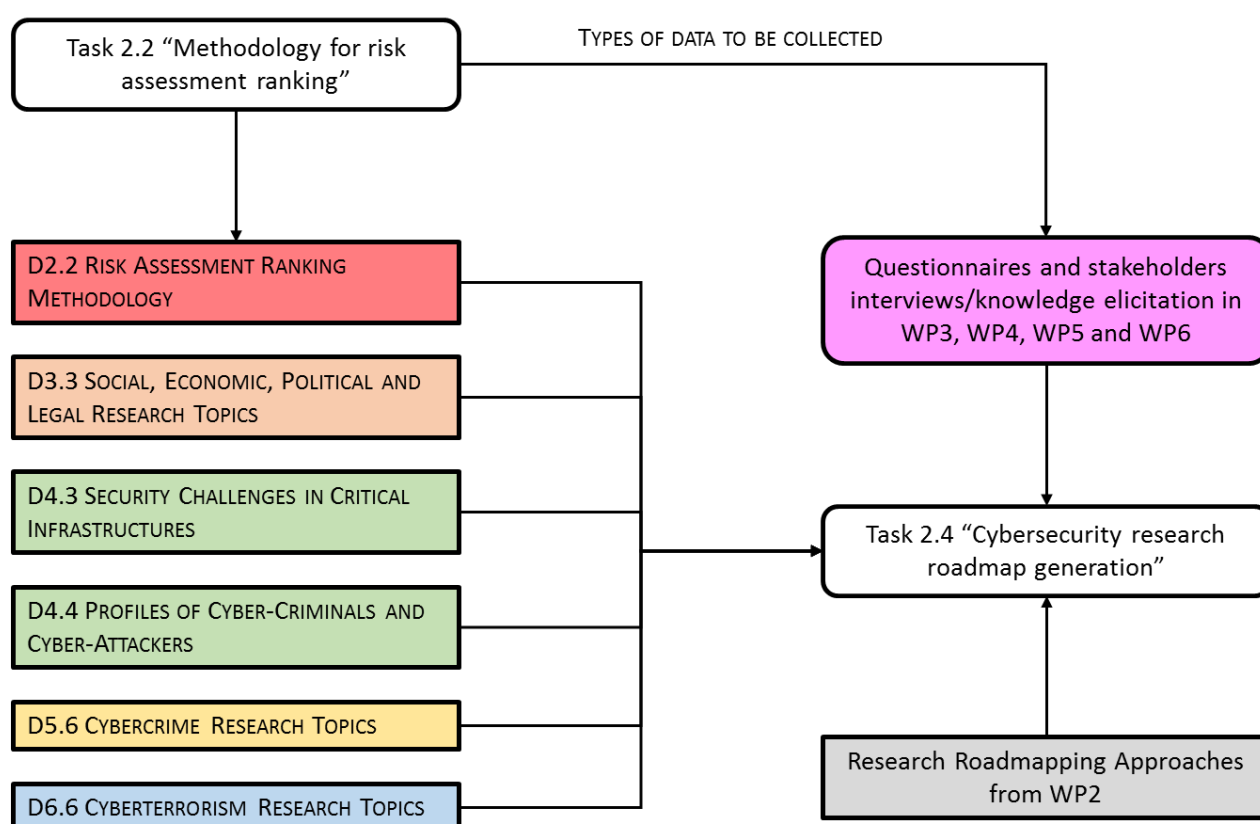
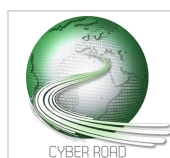


Figure 1 - Interactions between Task 2.2 and other CyberROAD tasks and outputs

In particular the proposed risk ranking methodology is the last step of the roadmapping methodology developed in WP2 (see section 6 for more details).



## 2 GENERAL APPROACH TO RISK ASSESSMENT

### 2.1 INTRODUCTION

**Risk** can be defined as the combination of the **probability** of an event and its **consequences**<sup>1</sup>. Or risk can be evaluated as the product of hazardous event and the frequency, or probability of occurrence.

What do we mean when we categorise something as risky, or very risky, or slightly risky? Driving an old car with poor steering, bald tyres and faulty brakes is inherently more risky than driving a brand new car in perfect condition, given similar speeds and circumstances. This is because the probability of having an accident is greater. Probability is, therefore, a part of the concept of risk.

However, the probability of having an accident by falling off a low ladder may be just the same as the probability of falling off a high ladder; climbing a high ladder is nevertheless riskier because the consequences are potentially much more severe.

The hazards and threats may be categorised as leading to a number of types of risks. These may include:

- Environmental risk, which includes risks of damage to the natural or built environment and covers all environmental media (land, air and water). Examples include risk posed by landfilling and other geological waste disposal methods.
- Technical risk, which includes risks posed by using new, often untested, equipment or methods (potentially yielding a higher rate of return) as opposed to known methods.
- Health and safety risks, i.e. those posed by hazards at work and to third parties.
- Economic, finance and asset risks including risks associated with insurance or loss of income if business needs to be shut down.
- Loss of business credibility.
- Public relations risk involving credibility and adverse public opinion.
- In addition there can be social, religion and cultural and others.

These risks are commonly inter-related. For example, health and safety issues could affect finance, public relations, and the environment and it is therefore important to approach risk management from a holistic (or systems) point of view.

There are several methods for assessing risk which can be categorised as qualitative or quantitative.

Formal risk assessment can range from simple qualitative classification into categories such as “High”, “Medium” and “Low”, through to the quantitative by use of mathematical models, which can vary from deterministic to the use of probabilistic/ stochastic models.

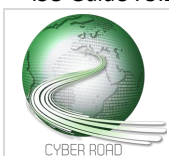
In risk assessment the threat to the system must be considered as coming from within the company/organisation as well as from external environment.

Many risks can be readily assessed using qualitative methods, or even “gut feeling” without resorting to more detailed and time consuming quantitative risk assessment methods.

### 2.2 QUALITATIVE RISK ASSESSMENT

The simple qualitative risk assessment approach is based on identifying threats/hazards and ranking the estimated risk from the perceived likelihood and consequence of each. For example, scales such as those shown in table below can be devised to categorise the likelihood and consequence.

<sup>1</sup> ISO Guide 73:2009 Risk management -- Vocabulary



Risk can then be categorised as “low”, “medium” or “high” using the “Boston Square” method.

The Boston square approach has the advantage of relative simplicity but is very subjective and open to bias.

Quantitative techniques may be more appropriate in several circumstances, including:

- when there are concerns that significant hazards may be overlooked by qualitative approaches;
- where there may be uncertainties over the likelihood or consequence (or both) of a system going wrong and where quantifying these may reduce uncertainty;
- where qualitative assessments indicate a significant number of risks in a system, hence there is a need to prioritise risk reduction or mitigation work using more robust techniques, especially when significant levels of spending are required.

In the qualitative methods the scale of likelihood and consequence must be devised to represent the system under investigation. The likelihood scale can be devised as shown below in Table 1. The numerical values can be obtained from some historical data or elicited from experts or a combination of both approaches.

Table 1 - Likelihood scale

Scale of Likelihood	Likelihood of occurrence
High	1 per day
Medium	1 per week
Low	unexpected

Similarly, the scale for consequence of threats/hazards can be defined (Table 2).

Table 2 - Consequence scale

Level	Consequence definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.

Combining the likelihood and consequence scales, a Boston Square as shown in Table 3 can be established. Allocating likelihood scale as 1 for high 0.5 for medium and 0.1 for low and for consequence scale 100 for high, 50 for medium and 10 for low, Boston square shown below is formed multiplying the row and column values. Considering the high risk events as ranging from 50+ to 100, medium risk from 10+ to 50 and low risk below 10, the risk of any threat event leading to consequence with assumed likelihood can be estimated from the derived Boston Square.



Table 3 - Risk Matrix (Boston square)

		Potential consequence		
		Low(10)	Medium (50)	High(100)
Threat likelihood	High (1)	10	50	100
	Medium (0.5)	5	25	50
	Low (0.1)	1	5	10

## 2.3 QUANTITATIVE RISK ASSESSMENT

The quantitative risk analysis techniques available are generally those that have been used in health and safety risk assessment for some time. However, it is important to understand some of the limitations of these techniques when applied to environmental risk assessment. These are discussed in some detail in the following section.

The more detailed risk assessments may be based upon a scenario approach or be based upon Monte Carlo simulation (probabilistic systems assessment (PSA) approach).

## 2.4 PROPOSED METHODOLOGY

The overall methodology is presented in Figure 2 below and can be used in both qualitative and quantitative assessment. Further details of each step follow:

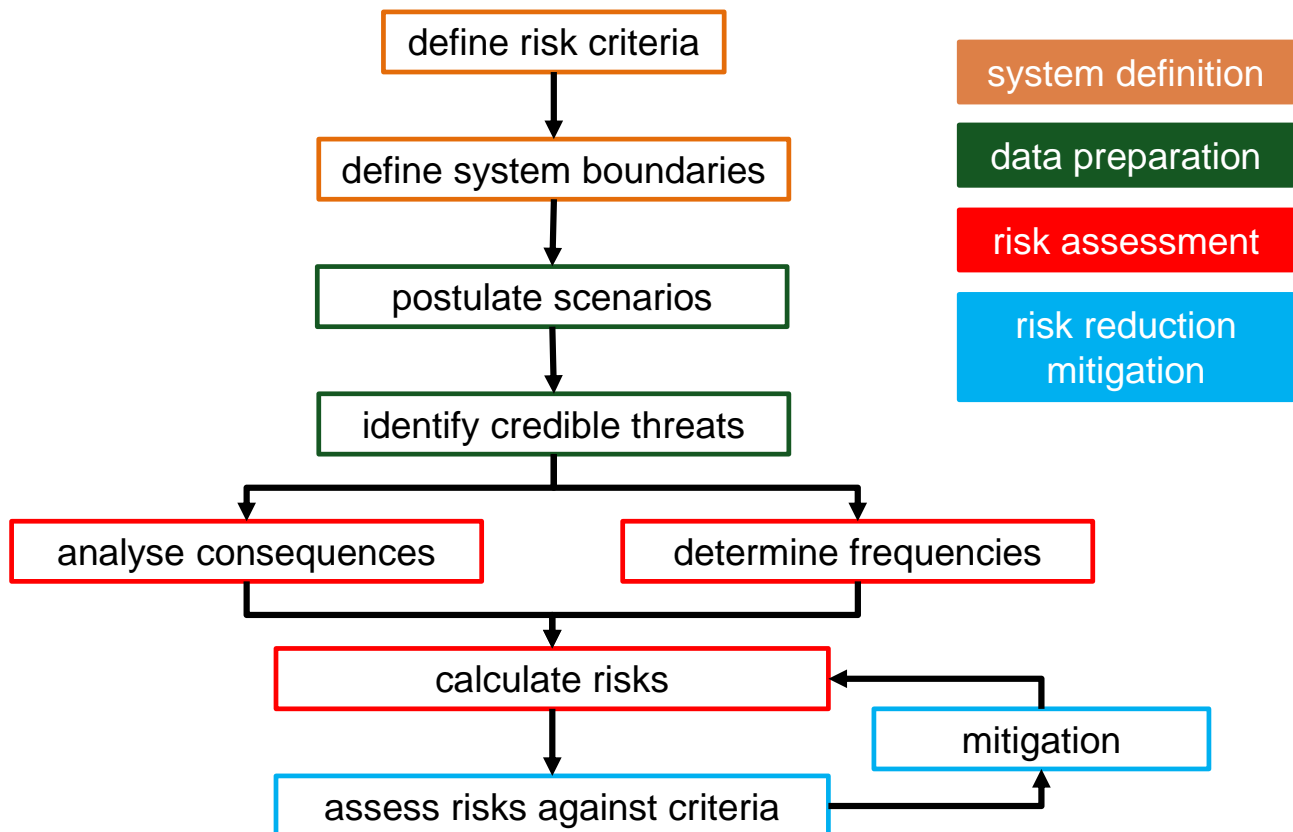


Figure 2 - Proposed assessment methodology



### 2.4.1 RISK CRITERIA

The first step is to check and agree on applicable criteria, i.e. criteria assessing harm and acceptability of risks. Before embarking on a Risk Assessment, it is important to be clear what criteria will be used to judge the tolerability of the predicted risks.

Authoritative guidance on risk criteria is limited, and can rarely be directly applied. The numerical risk targets tentatively suggested in guidance such as that published by the UK Health and Safety Executive<sup>2</sup> (HSE) are all too often quoted out of context, and applied without sufficient consideration of their applicability to other systems or plant. The main factors to be considered include:

- **General Principles of Risk Control.** Many assessments consider only the limitation of risk - i.e. the requirement that the predicted values should be below some numerical limit
- **The Risk Envelope.** Defining the risks to which any criterion is intended to apply is closely linked with the definition of physical and operational boundaries, as described above. It may also involve the question of risk “ownership”, i.e. establishing what risks should properly be associated with the proposed system. The criteria can be considered as relative or absolute.
- **Average and Peak Risk.** To ensure that the risk from a process is tolerable both the peak risk and risk when averaged over operation should be within the risk envelope.
- **Risk Perception.** The extent to which people or organisation will tolerate any particular source of risk depends not just on the numerical level of risk which it poses (even supposing that this can be objectively evaluated). Studies have repeatedly demonstrated that social, psychological and cultural factors have a major influence on risk acceptance.

### 2.4.2 DEFINITION OF SYSTEM BOUNDARIES

The second step deals with defining boundaries of system under investigation and any interaction with other systems. In any risk assessment it is essential to define precisely the physical and operational boundaries of the system being assessed. Defining the physical boundaries includes for example the decision to what granularity to represent the network system.

Defining the operational boundaries involves deciding on the phases of a system lifecycle and the processes to be considered. Most studies concentrate on normal operating conditions, but, commissioning the system, inspection, maintenance, repair may be equally important.

### 2.4.3 DATA COLLECTION

The third step is to collect data for the analysis (system description, operational procedure etc.). Data collection and analysis is a major task in any assessment and it is particularly important to the successful completion of a Quantified Risk Assessment (QRA).

The data requirements range from simple system operating diagrams, including historic data required to establish frequencies of failures and accidents. Data may be required on human behaviour and reliability as well as system reliability.

The quality of the risk assessment relies on the quality of the data collected.

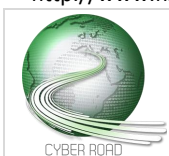
### 2.4.4 IDENTIFICATION OF THREATS/HAZARDS

The fourth step is aimed at identifying threats/hazards associated with the system under investigation. The success of any Risk Assessment depends on comprehensive identification of these potential hazards/threats.

These threats can fall into two categories:

---

<sup>2</sup> <http://www.hse.gov.uk/>



1. Internal threats/hazards - Hazards intrinsic to the organization or activity under consideration
2. External threats/hazards - Hazards imposed by external factors

At its simplest, hazard identification means establishing what could go wrong with the site, system or procedure being considered. Therefore there is a need to identify all the ways in which the assets and their protective procedures/systems involved may fail either through malicious activities or through human errors.

A variety of more or less formalised hazard identification techniques have been developed to ensure that identification is as comprehensive as possible. The simplest example is the use of pre-defined checklists. These are quick and easy to apply, but have the danger of limiting the range of thought - if a hazard is not on the checklist the assessor may not look for it.

More thorough, but more time-consuming and costly approaches include structured techniques based on group sessions such as Hazard and Operability Study<sup>3</sup> (HAZOP) or Failure Mode and Effect Analysis<sup>4</sup> (FMEA).

The advantage of a group session is that the interactions between participants with differing experience and expertise tend to promote broader thinking, and take better account of the interfaces between subsystems and activities. Such sessions can also have more immediate and wider benefits in terms of the overall safety culture, by promoting awareness of existing hazards and understanding of differing viewpoints.

#### **2.4.5 CONSEQUENCE ANALYSIS**

The fifth step deals with the evaluation of the consequences of any threats on a company or business and the consequences of the protective system barrier failure due to the cyberattack on the integrity of the assets of the organisation. Such studies can determine the impact of accidents on personnel, equipment, and the environment.

For the technical and natural hazards numerous mathematical/computational models are available to determine the severity of consequences, while for cyber-terrorism and cyber-crime, experience from past events is the most reliable source of information.

#### **2.4.6 ESTIMATION OF EVENT/THREAT FREQUENCIES**

The sixth step is to determine frequencies of events and failure probability for each scenario.

A number of approaches may be adopted to obtain estimates of the frequency of initial threats/ hazardous events. The main methods are:

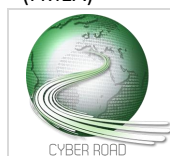
- an analysis of appropriate historical data applicable to the given system and event;
- fault tree analysis (using component and human reliability data), when a combination of failure events is required;
- formalised techniques of eliciting expert judgements can be applied when the historical data is very limited.

#### **2.4.7 RISK ESTIMATES**

Having completed the previous steps, it is then necessary to determine the risks and assess the acceptability of these risks against criteria and review the option for risk reduction. Having established the factors influencing the risk (consequence and frequency), these factors must then be combined to produce an overall risk estimate for each hazard. At the lowest level this may be simply a summation of the products

<sup>3</sup> See for example IEC 61882:2001 "Hazard and operability studies (HAZOP studies) - Application guide"

<sup>4</sup> See for example IEC 60812:2006 "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)"



of the various consequences and their probabilities of occurrence, using for example an event tree approach. In more complex cases a theoretical model of system behaviour using a deterministic or stochastic technique is applied.

#### **2.4.8 TREATMENT OF UNCERTAINTY AND BIAS**

Uncertainties will arise throughout a quantified risk analysis as a result of sparse data, simplifications and assumptions in the models used, the interpretations and representations of the processes being modelled and in the results generated. In general, the greater the uncertainty, the greater will be the variability in risk estimates for any given situation.

Uncertainty may be regarded as a lack of complete knowledge about the true nature or extent of some effects on the behaviour of a system.

Treatment of uncertainty is now well understood, the effects of bias are not. Bias may be regarded as an effect which leads to a systematic distortion in the understanding of system behaviour. Thus a particular process, or particular interactions between processes, may be omitted or an inappropriate model may be used.

The effects of bias are more difficult to quantify, since by definition the system representation does not include the processes generating the bias. Bias cannot be investigated by changing model inputs, but only by using alternative conceptual models.

#### **2.4.9 RISK MITIGATION/REDUCTION**

Risk is the product of likelihood and consequence. Then to reduce the risk one can reduce the likelihood of risk (frequency of occurrence) or changing the system design to reduce the impact. Other methods will involve:

- elimination;
- substitution;
- control;
- improving the ability for recovery from an occurrence;
- transferring the risk to another entity (e.g. an insurance company).

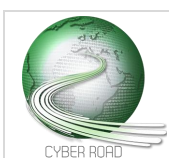
#### **2.4.10 ELICITATION FROM EXPERTS**

The risk methodology outlined above relies on risk values elicited from experts. It is suggested that this data collection could take place at the same time that the research topics are elicited from experts. Alternatively this data can be gathered from the same experts in a separate session. The elicitation can be conducted with individual experts separately or by means of group elicitation.

The advantage of a group session is that the interactions between participants with differing experience and expertise tend to promote broader thinking, and take better account of the interfaces between subsystems and activities. Such sessions can also have more immediate and wider benefits in terms of the overall safety culture, by promoting awareness of existing hazards and understanding of differing viewpoints.

In the formal group elicitation, the format of such sessions is usually based on the application of a set of prompts (keywords) to some structured breakdown of the system or process being considered. Thus for example, keywords such as NOT DONE or MISUNDERSTOOD can be applied to each task in a procedure to prompt participants' thinking about how it might go wrong. The structured format promotes comprehensive consideration of the problem, whilst the keywords encourage creative thinking.

The elicitation from experts can concentrate on individual value of risk per research topic or on risk including uncertainty.



### 3 APPROACHES TO ELICITATION WITH UNCERTAINTY

Uncertainties will arise throughout a quantified risk analysis as a result of sparse data, simplifications and assumptions in the models used, the interpretations and representations of the processes being modelled and in the results generated. In general the greater the uncertainty, the greater will be the variability in risk estimates for any given situation.

Uncertainty may be regarded as a lack of complete knowledge about the true nature or extent of some effect on the behaviour of a system or process, or in the case of data elicited from experts, from each expert's view and experience of the process.

The treatment of uncertainty in risk assessment is becoming increasingly commonplace, but generally requires considerable resources to be performed rigorously. Treatments of uncertainty can broadly be separated into two groups:

1. Methods in which risk is derived by summing the contributions to the total risk from all significant event types. In these methods the event probabilities and outcomes are derived separately.
2. Methods in which risk is derived directly from a 'complete' representation of the system under all possible conditions. In these methods the probability of any particular event and any associated uncertainty is implicitly accounted for in the distributions of possible values assigned to its inputs.

Examples are:

- Monte Carlo sampling methods;
- direct integration methods.

Typically the proper treatment of uncertainty will involve

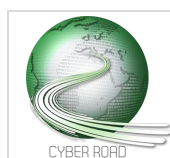
- characterising the full range of system behaviour in a conceptual model, or models, of the system;
- establishing the parameters which influence system behaviour and their ranges of possible values;
- investigating the behaviour of the system over the range of inputs;
- testing the results of the investigation for completeness;
- analysis of the results to establish which parameters contribute most to the variability in system behaviour;
- derivation of the risk under uncertainty.

Using a Monte Carlo approach, this process typically involves the development of a stochastic system representation of all the interacting processes. This model would be run many times, sampling its inputs from specified distributions of parameter value ranges. The results from this stochastic model must then be statistically analysed to ensure the results from the model are converged, to produce the output distribution and risk calculations.

In addition, sensitivity analysis may be performed to identify those input parameters which contributed most to the variability in the output. These so called sensitive parameters may then be analysed in more detail in order to ensure the results are reasonable, and the model is behaving correctly under extreme conditions.

The uncertainty treatment in the case of a lack of mathematical model is to elicit the risk values by asking the experts to provide the values by means of 'subjective' Probability Density Function (PDF) reflecting the expert belief regarding the value range. The experts can also judge the shape of the PDF.

The experts can select the PDF from a range of functions (see Table 4).



**Table 4 - Example of Probability Distribution Function (PDF)**

PDF	Representative values	PDF	Representative values
Uniform	Min, Max	Normal	Mean, Standard Deviation (SD)
Triangular	Min, Max, Mode	Exponential	Min, Mean
Beta	Min, Max, Mean, SD	Gamma	Min>0, quantile

In practice Uniform PDF is quite useful, where only minimum and maximum values are available. A Triangular distribution function is also very useful since it can be defined by three parameters, minimum, most likely and maximum, and has the advantage that it is easy to visualise and understand.

Expert elicitation sessions should be prepared and conducted in such a way as to reduce the bias in subjective judgement and errors in the result outcome. The participants in the elicitation exercise should be provided with a briefing document outlining the elicitation procedure and stressed that consensus is not the main goal of the process. The elicitation of risk value should follow the methodology outlined in previous chapter. The risk value from each expert can be a single value or a PDF parameters depending on type of risk considered. The elicitation session is normally followed by post-elicitation discussion and feedback analysis of outcome and aggregate of results.

### **3.1 AGGREGATE OF MULTIPLE UNCERTAIN OUTCOMES**

The output from the elicitation of risk values must be checked for reality and outliers. Reality checks can be agreed in post elicitation session, outliers eliminated during result analysis.

The simplest method of combining the results from individual experts is by giving all the experts equal weight. In the case of single values, these can be aggregated using an arithmetic mean (where N is the number of experts).

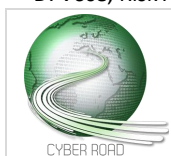
$$Risk = \sum_i \frac{Risk_i}{N}$$

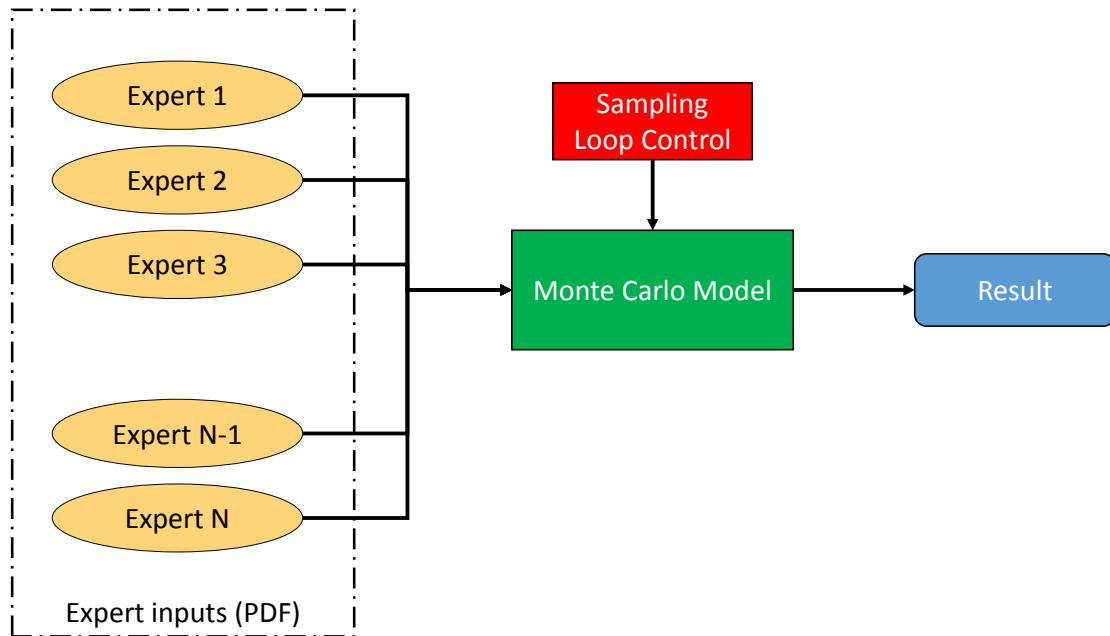
Here in the case of multiple experts each providing PDF's there is no best method to combine them into a single PDF. Therefore to explore the uncertainty in output from experts the individual PDF elicited by experts are combined using a simple stochastic model to produce a single combined probability distribution and hence mean and measure of spread for the risk value.

Two approaches can be used to combine the results into single PDF <sup>5</sup>

1. Random Monte Carlo,
2. Stratified sampling based on Latin Hypercube.

<sup>5</sup> D. Vose, Risk Analysis: A Quantitative Guide, 3rd Edition, 2008, J. Wiley





**Figure 3 - Method of combining multiple PDF's from Experts**

An example of combining multiple PDF's is shown on the Figure 3 above. Here the Monte Carlo is based on sampling of inputs from the expert PDF's (as deterministic value) and combining each sample arithmetically hundreds or thousands of times, the resulting output will be represented by single PDF. To speed up the number of runs needed for convergence a stratified sampling method e.g. Latin Hypercube can be used. With such method correlation between parameter inputs is feasible.

The above method can be used not only for the derived Risk PDF's but also for any other parameters elicited from experts.

## 4 PROPOSED RISK RANKING

Task 2.2 deals with a method for ranking Research Topics associated with cyber-crime and cyber-terrorism. The document starts from the hypothesis that the data collected on these research topics from stakeholders will be subjective, and not of sufficient quality to consider a quantitative approach. Furthermore the lack of sufficiently verified data on frequency-severity of cyberattacks make it difficult to use sophisticated techniques. Therefore the method proposed is based on Boston Square method. If after collecting the initial data it will be apparent that some quantitative approach will be feasible, an approach using some uncertainty theory as described in section 3 will be tested and if successful implemented.

### 4.1 OVERALL APPROACH FOR RESEARCH RANKING PRIORITISATION

The overall approach is presented in Figure 4 below.

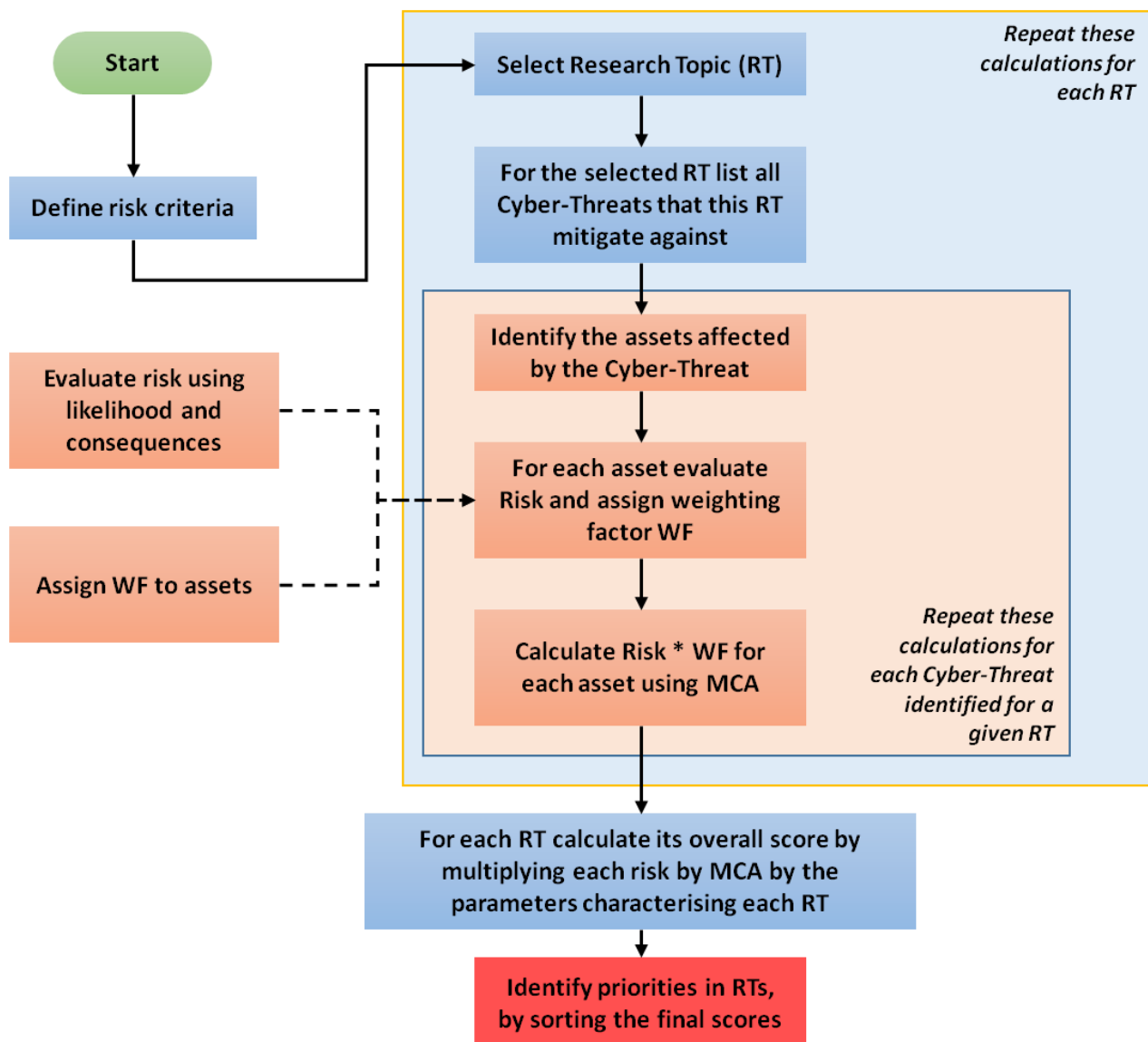


Figure 4 Overall methodology for Prioritisation of research topics for cyber-crime and cyber-terrorism

The method follows several steps as shown in the flow chart in Figure 4 above:



- define criteria for assessing the priorities for cyber research;
- select research topic RT;
- create a list of Cyber Threats (CT);
- create a list of assets affected by each CT;
- for each asset calculate risks;
- score each RT to provide ranking prioritisation.

These steps will be now explained in the following sections.

#### 4.1.1 DEFINE CRITERIA FOR ASSESSING THE PRIORITIES FOR CYBER RESEARCH AND ITS BOUNDARY AND LIMITS

Different criteria could be considered, however criteria based on risk allow cyber research priority to be based on the level of harm that such cyber activities can inflict on a society. As outlined in previous sections, the extent of the study should be defined. The system under assessment is very large which includes organization, industrial companies, government bodies and public and private infrastructures, each containing unlimited subsystem. It will be impossible in this project to consider all. To facilitate the present task it is suggested that the **scenario-based** approach should be adopted, where the system under investigation will be represented by a limited set of cyber-crime and/or cyber-terrorism areas (the roadmapping methodology developed in WP2 goes along these lines). The number and types of cyber-crime topics will be elicited from stakeholders and agreed with project partners in Task 2.3.

#### 4.1.2 SELECT RESEARCH TOPIC RT

The Research Topics (RT) collected from experts and project partners, via interviews and questionnaires, should be checked for uniqueness and set as list. Then each RT is assessed separately.

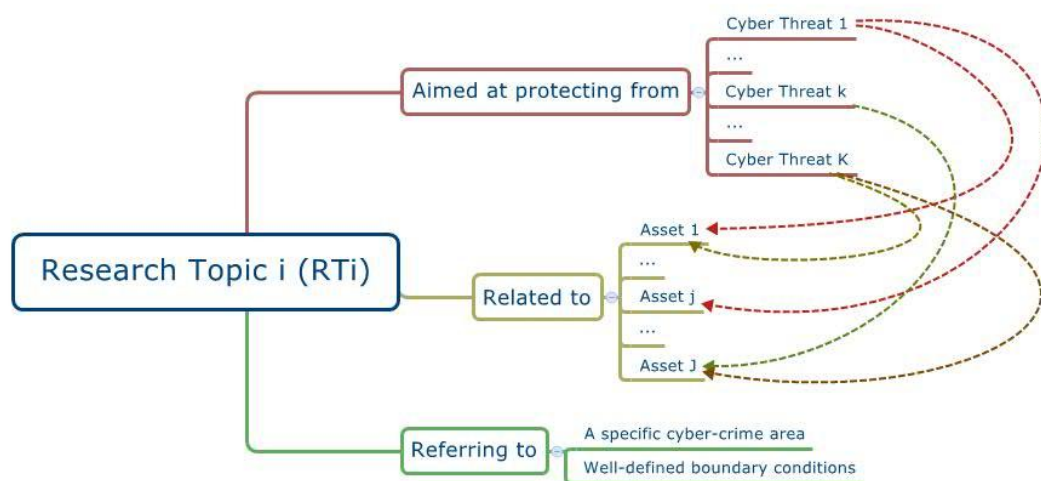


Figure 5 - Relationship between Research topic, threats, assets and risk

A Research Topic can be associated with one or more Cyber Threats (CT) which can affect one or several assets and each CT can give rise to risk of different types e.g., financial, reputational, environmental, political etc. which can affect several assets (see Figure 5).

#### 4.1.3 CREATE A LIST OF CYBER THREATS

The list of possible Cyber-Threats (CT) and the related affected assets is expected to be generated by the work of the 4 specific work-packages of the CyberROAD project:

- WP3 - Social, Economic, Political and Legal Scenario;
- WP4 - Technological Scenario;
- WP5 - Cybercrime



- WP6 - Cyber-terrorism.

Then the CT to be considered in the ranking exercise will be identified and used in the Tasks 2.3 “Supervision and harmonisation of information collection and assessment” and 2.4 “Cyber-security roadmap generation”, respectively.

#### 4.1.4 CREATE A LIST OF ASSETS AFFECTED BY EACH CT

The following step is to create a list of assets affected by each Cyber-Threat. The identification of assets is strongly dependent on considered organisations but typically includes **tangible assets** (e.g. funds and financial instruments, infrastructure, and production capabilities) as well as **intangible assets** (e.g. reputation).

As an example we can consider a commercial organisation. Every business or organisation possesses assets, some of which are physical, others fall under the category of information and computer systems.

The physical assets can be: computer equipment (e.g. mainframe computers, servers, desktops and notebook computers, etc.), communication equipment (modems, routers, firewalls, etc.), storage media, other technical equipment, etc.

The information assets can be company information, procedures, intellectual property rights. These will include databases with critical information about the organisation, like finances, marketing, client information etc. Other critical information can be stored in data files which also should be protected.

Software assets can fall into two categories, system software and application software.

Some of the assets can be classified as critical. Critical assets are assets which if destroyed by cyber-attacks or infiltrated by malicious software, could cause business to suffer substantial financial losses. These assets must be protected against such cyber-attacks.

The weakness or gap in protection efforts as applied to the asset from internal or external attacks is considered asset vulnerability. The more that critical asset is vulnerable to cyber threat, the risk to asset increases.

#### 4.1.5 CALCULATE ALL THE RISKS USING BOSTON SQUARE

The next step is to calculate, for each asset, all the risks using Boston square from likelihood and consequences elicited from experts. An example of tangible and intangible cyber risks is shown in Figure 6. The tangible risks are easier to assess and their impact can be monetarily evaluated whereas intangible risks are assessed more subjectively.



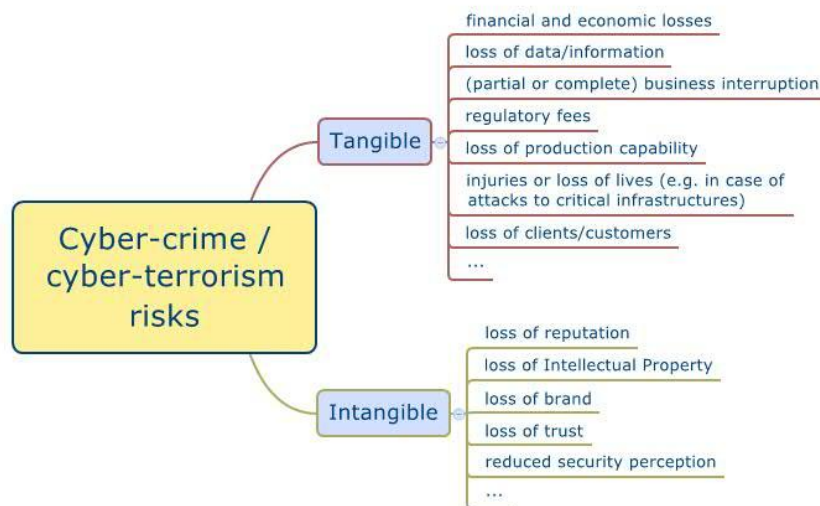


Figure 6 - Example of tangible and intangible cyber risks

It is necessary to estimate the risk for each asset, keeping the results for each risk type separately (e.g. financial, health & safety, technical). The scales for likelihood and consequence and hence risk are assigned here for illustration purpose (see Table 5). These should be defined and agreed with the stakeholders.

Table 5 - Likelihood scale

Scale of Likelihood		Likelihood of occurrence
Highly probable/Likely	10	1 per day - Very likely target
Medium/Possible	5	1 per week - Possible target
Low/Remote	2	1 per month - Remote target
Negligible/Unlikely	1	Unexpected - Unlikely target

The consequence from any threat can be estimated using the scale presented in Table 6.

Table 6 - Consequence scale

Level		Consequence on assets
High/Severe	10	Irreparable harm to the company (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury
Medium/Major	5	Significant harm (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low/Moderate	2	Moderate harm (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.
Minor	1	Very unlikely to cause any harm to the company or caused injuries

The risk from a Cyber Threat CT posed to each asset is calculated using Boston Square method, for which a numerical values for likelihood and consequence will be required. These values will be obtained by eliciting them from project partners and/or from stakeholders.



After having set the values obtained for likelihood and consequence for a given threat, asset and risk type, a risk level is estimated from a risk matrix see Table 7 (where cells in red correspond to HIGH risk, yellow to MEDIUM risk and GREEN to low risk).

Table 7 - Example of a risk matrix (for each type of risk)

Likelihood of threat(s)	Highly probable/Likely	10	20	50	100
	Medium/Possible	5	10	25	50
	Low/Remote	2	4	10	20
	Negligible/Unlikely	1	2	5	10
		Minor	Low/Moderate	Medium/Major	High/Severe
Consequences (severity) of RT associated threat(s)					

When assessing the risk each aspect of risk e.g. financial risk, health & safety, environmental or reputational are evaluated separately, since each can have different metrics and as such cannot be added directly. For example **Environmental** risk can be measured using loss of habitat, **Health and Safety** using mortality or degree of injuries and **Financial** risk using monetary value. Therefore to be able to combine these different types of risk, the risks should be brought to a common metric e.g. monetary.

In most cases combining different types of risk is quite complex. Nevertheless since the risk based approach for risk ranking is very subjective and based on very subjective data, it is suggested that some simple approach based on **Multi Criteria Analysis (MCA)** should be sufficient to apply, to combine different types of risk. Each risk type is scored from 1 to 100 (in current example).

Using MCA, each risk type will require to be multiplied by a weighting factor (WF) to provide a factor for a given risk type representing a relative preference. Thus if in an assessment the a financial risk is preferred by a factor Fp over an environmental risk then WF is set to Fp. The weighting factor value should also be obtained by elicitation from experts. The approach is in line with the context in which ranking of Research Topics is done.

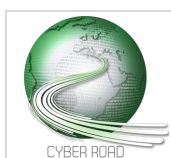
Thus MCA is a method for considering complex problems that can be characterised by different objectives (financial and non-monetary). Here MCA is applied for aggregation of risks of different type by multiplying each risk by corresponding weighting factor such that risks of different type can be added together to form a single value corresponding to a given research topic.

A **risk ranking matrix** is the main output of the analysis. Each research topic RT[i] in the table contains all the risk types and weighting factors applicable to its threats. The resulting matrix could be a sparse matrix since for some RT[i] certain risk/weighting factor could not be applicable. The decision makers then have a task of **reviewing** it to the extent to which the objectives are satisfied by the entries in the matrix. This is more an intuitive process of data. It is speedy and effective, but it also may lead to assumption which cannot be justified and can lead to incorrect ranking. Therefore at this stage the results obtained should be subjected to a reality check and sensitivity analysis to assess how the assumptions affect the overall results.

The **overall score** RW[i], for each RT is computed according to the following formula:

$$RW[i] = \sum_j \sum_m \sum_k RS[j, m, k] * WF[k]$$

where:



- $RS[j, m, k]$  is the value of the risk when considering the Research Topic  $RT[i]$  and the Cyber-Threat  $CT[j]$  associated to  $RT[i]$  for a given asset  $A[m]$  and a given type of risk  $k$
- $WF[k]$  is the weighting factor applied to the risk of type  $k$

#### 4.1.6 SCORE EACH RESEARCH TOPIC TO PROVIDE RANKING PRIORITISATION

Ranking means arranging in order with regards to some common criteria. These criteria could be based on risk severity. In the event that a ranking of research topics is based on the value of risk criteria then ranking can be achieved by simply sorting  $RW[i]$  from highest to lowest value.

However to provide a more general method for ranking research topics  $RW[i]$  can be provided with **additional attributes not related to risk**. These can be associated with factors related to maturity of research topic (basic or final stage), costs associated with its development, complexity etc. These attributes can also be elicited from the stakeholders and system users. Some examples of such attributes are shown in Figure 7.

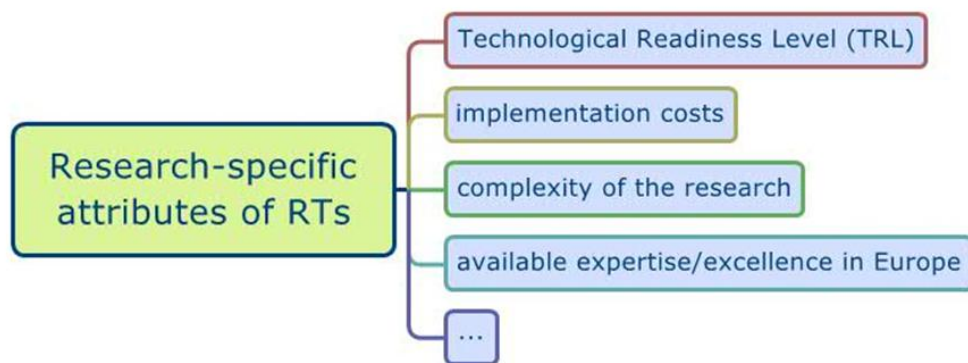


Figure 7 - Example of Research Topic specific attributes

As a first example of attributes to be used is the **Technology Readiness Level (TRL)**. The Technology Readiness Level (TRL) scale was developed during the 1970-80's. The National Aeronautics and Space Administration (NASA) introduced the scale as *"a discipline-independent, program figure of merit (FOM) to allow more effective assessment of, and communication regarding the maturity of new technologies"*<sup>6</sup>. Many other definition of TRL exist, including the NASA version with 9 levels<sup>7</sup>, the adaptation to specific needs of the US-Department of Health and Human services<sup>8</sup>, etc.

In particular, The European Commission has introduced, in Horizon 2020 programme, the Technology Readiness Level (TRL) definition reported in Table 8.

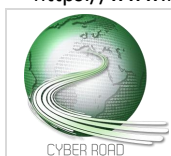
Table 8 - Technology Readiness Level (TRL)

Technology Readiness Level (TRL)	Definition
TRL 1	basic principles observed
TRL 2	technology concept formulated

<sup>6</sup> Mankins JC (2009), Technology readiness assessments: A retrospective, Acta Astronautica 65 1216–1223, Pergamon.

<sup>7</sup> US Department of Defence (2011), Technology Readiness Assessment (TRA)-guidance Washington

<sup>8</sup> <https://www.medicalcountermeasures.gov/federal-initiatives/guidance/integrated-trls.aspx>



TRL 3	experimental proof of concept
TRL 4	technology validated in lab
TRL 5	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7	system prototype demonstration in operational environment
TRL 8	system complete and qualified
TRL 9	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Hence it is possible to define a factor  $TRLf[i]$  applicable to a given Research Topic  $RT[i]$  which can represent distance of RT to the market as:

$$TRLf[i] = (\text{value of TRL of } RT[i])/9$$

Assuming that research topic which is nearer to completion i.e. with  $TRLf[i]$  nearer to one is preferred than one with lower  $TRLf$ . Hence If two research topics have the same risk value, RT nearer completion will have higher research ranking.

Hence for the i-th RT

$$RTV[i] = RW[i] * TRLf[i]$$

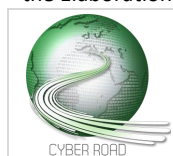
here  $RTV[i]$  is **modified scored** for given RT.

Other factors  $RTf[i]$  may be defined in a similar way, including the non-exhaustive list in Table 9.

Table 9 - Possible factors describing RTs

Possible factor	Description
Cost of the Research Topic relative to others	<p>The cost of a Research Topic relative to others can be estimated in terms of the number of projects the EU should fund for getting proper results.</p> <p>To this aim, two kinds of FP7 project types can be considered as unit of measurement:</p> <ul style="list-style-type: none"> <li>• Small or Medium Scale focused research project (STREP): typical duration 18-36 months, 6-15 participants, EU contribution 1-4 M€, with an average around 2 M€</li> <li>• Integrated Project (IP): typical duration 36-60 months, 10-40 participants, total EU contribution 4-25 M€, with an average around 10 M€</li> </ul>
Availability of competences in EU	Availability of competences in EU can be evaluated using a scale from 1 (minimum) to 5 (maximum)
Critical Research Topic	After defining a Critical RT as “any RT result (including equipment, skill, system, service, infrastructure, software or component) that is required by any organisation with a legal or contractual responsibility for cyber-security to properly perform its duties” <sup>9</sup> , it is possible to express it in a scale from 1 (minimum) to 5 (maximum)

<sup>9</sup> Inspired by the definition of Critical Technology introduced by the ETCETERA “Evaluation of Critical and Emerging Technologies for the Elaboration of a Security Research Agenda” project (7<sup>th</sup> Framework Programme, GA no. 261512)



So the final score of research topic will be calculated from RT risk value  $RW[i]$  and any agreed factors.

In general the RTV value will be calculated using

$$RTV[i] = RW[i] * RTCOEFF[i]$$

where

$$RTCOEFF[i] = (TRLf[i] + RTf[1] + RTf[2] + \dots)$$

where  $RTCOEFF[i]$  is general factor characterising the given Research Topic.

The ranking of research topic is obtained by sorting  $RTV[i]$  from highest to lower values.

An overall methodology for ranking Research Topic is presented in a flow chart in Figure 8 below.



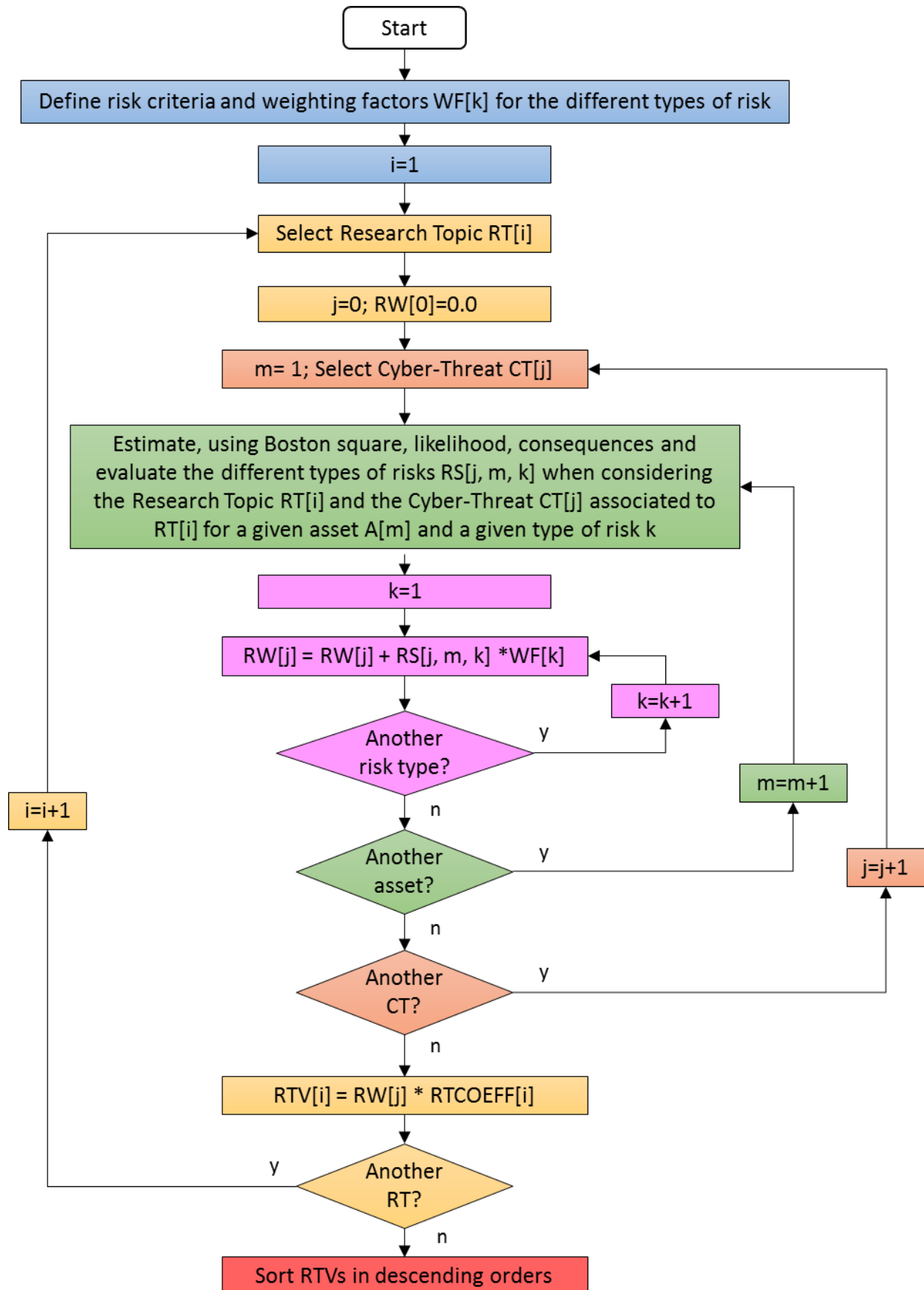


Figure 8 - The chart for ranking research topics

## 5 INTERACTION WITH CYBERROAD WP5

On the basis of the methodology developed in the previous sections, the following questions have been added to the WP5 survey #2 “Technology & Organisation” (see printouts from SurveyMonkey © screens in Figure 9, Figure 10 and Figure 11) to elicit risk knowledge from experts (see section 3):

ii. Using the likelihood scale provided what, according to your own experience, is the likelihood of the listed cyber threats occurring?

Scale of Likelihood		Likelihood of occurrence
Highly probable/Likely	10	1 per day - Very likely target
Medium/Possible	5	1 per week - Possible target
Low/Remote	2	1 per month - Remote target
Negligible/Unlikely	1	Unexpected - Unlikely target

Cyber threats (based on ENISA's Top 10 Emerging Threats):

	Highly probable/likely	Medium/possible	Low/remote	Negligible/unlikely
Malicious code: Worms/Trojans	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web-based attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web application attacks /injection attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Botnets	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Denial of service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exploit kits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data breaches	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Physical damage/theft /loss	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Insider threat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information leakage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Identity theft/fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber espionage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ransomware/ Rogueware/ Scareware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify)

Figure 9 - Question to estimate likelihood of cyber-threats

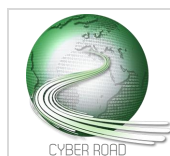
iii. What would be the consequences of a cyber attack on the following top targets from Survey #1

Level		Consequence on assets
High/Severe	10	Irreparable harm to the company (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury
Medium/Major	5	Significant harm (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low/Moderate	2	Moderate harm (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.
Minor	1	Very unlikely to cause any harm to the company or caused injuries

Use the Consequence Scale to rate an asset at risk.

	Consequence Scale
Personal data	High/severe (10) ▼
Critical information	Major/medium (5) ▼
Intellectual Property Rights	Low/moderate (2) ▼
On-Line services/Web applications	High/severe (10) ▼
Critical infrastructures	High/severe (10) ▼
Workstations (Users' equipment)	Minor (1) ▼
People (employees)	Low/moderate (2) ▼
Banking & financial service	High/severe (10) ▼
Payment systems	Major/medium (5) ▼
Mobile devices (tablets, smartphones)	High/severe (10) ▼

Figure 10 - Question to estimate the consequences of a cyber-attack





iv. Please quantify the importance of the following risks for your organisation.

	Very important	Important	Medium importance	Low importance	Negligible importance
Direct financial losses & damage (money stolen from accounts, regulatory fees, loss of clients, business, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Indirect financial losses (loss of reputation, brand, trust, missed business opportunities, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health & safety	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Environmental	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 11 - Question to estimate the importance of risks

## 6 RISK-BASED RANKING AND THE ROADMAPPING PROCESS

This risk-based ranking methodology is fully integrated in the road-mapping process developed in the first reporting period within the framework of the WP2 activities that is described in the following documents

- “Creation of Roadmaps based on Scenario Analysis” (Slides)<sup>10</sup>
- “Tutorial on Scenario Analysis & Roadmapping”<sup>11</sup>

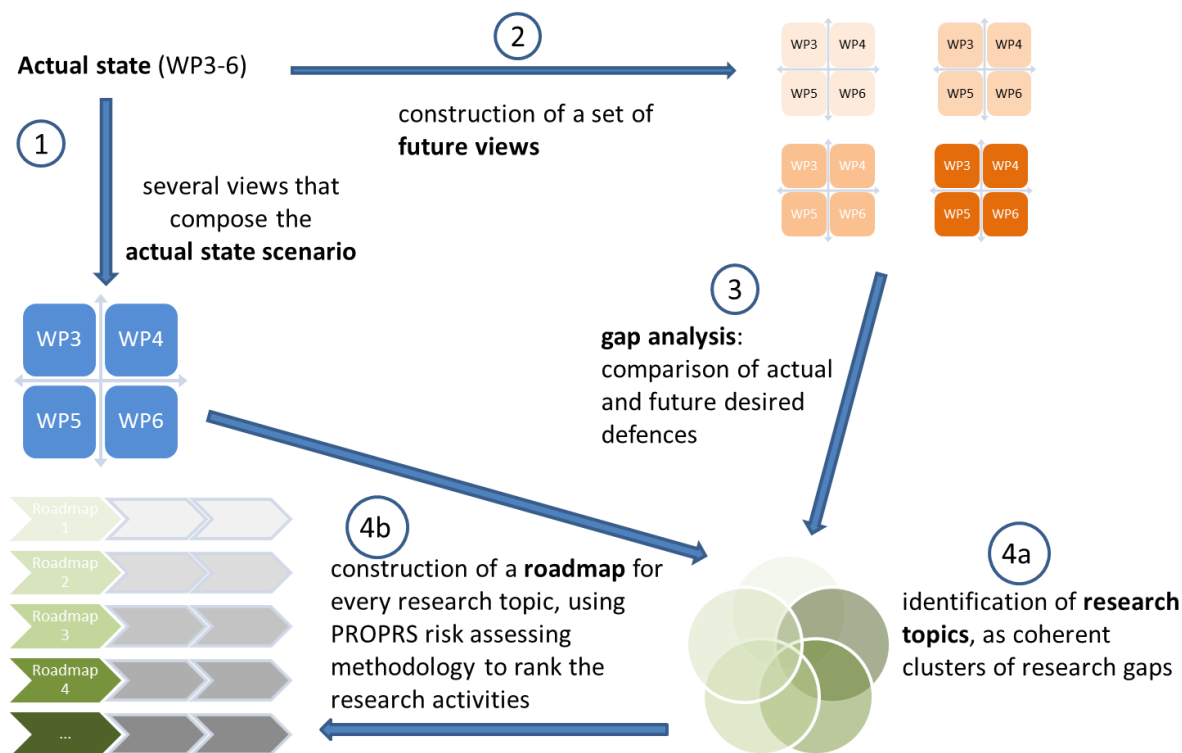


Figure 12 - Roadmap creation based on scenario analysis

As described in Figure 12, the roadmapping creation is based on the following steps:

1. generation of actual scenarios, each one composed by several views describing the actual state of cyber-crime and cyber-terrorism, i.e. the whole set of technological, social, economic and political conditions that define the context of cybercrime (CC) and of cyber-terrorism (CT), and the corresponding specific threats and defences;
2. construction of a set of future views (scenarios);
3. identification of the gaps;
4. identification and ranking of the research topics necessary to fill the gaps for each scenario
  - a. identification of the research topics;
  - b. **rank the research topics according to the risk-based methodology** defined in this document.

<sup>10</sup> <https://nue.diee.unica.it/public.php?service=files&t=c081e0bfaf0463ccdba1992327973ade>

<sup>11</sup> <https://nue.diee.unica.it/public.php?service=files&t=5389229a0f6bf9de6276446c0b12467c>

## 7 EVOLUTION OF THE RANKING OVER TIME

---

As defined in the roadmapping methodology developed in WP2, a research topic is a set of research actions required to address the research topic gaps. The identified research actions are then put into a clear time frame.

This means that if one or more research actions are addressed successfully in the research arena then most likely one or more of the following event could happen:

- the TRL of that Research Action changes (e.g. from TRL3 to TRL 8);
- the likelihood of occurrence of the addressed threats is reduced;
- the consequences on the threatened assets are mitigated.

If the above happens, it is then possible to repeat the methodology with the new values and update the ranking consequently.

The new ranking may, for example, highlight

- the need to focus on other research actions within the same research topic;
- and/or to modify the set of research actions required to fill the remaining gaps of the research topic;
- and/or to concentrate attention and funding on another research topic.



## APPENDIX 1 - MCA EXAMPLE

To clarify the approach we present here below a very simplified example. We consider the critical infrastructure world (railway in particular), focusing on the cyber-terrorism problem and on 2 specific Research Topics (RT):

RT1. ICT tools to protect from intrusion in railway command and control systems to interrupt circulation

RT2. ICT tools to protect from intrusion into social media to generate panic in railway stations with false information

The threat associated to RT1 is the intrusion in the command and control system affecting the following main assets: the quality of service. The threat associated to RT2 is the intrusion in social media affecting the following main asset: the railway passengers.

We also consider 2 different risk categories:

1. financial risk
2. health & safety

It is assumed that the stakeholders using Table 5, Table 6 and Table 7 - after a survey and an averaging exercise - decide that

- RT1 associated threat has
  - low likelihood and high financial consequences
  - and low likelihood and low health & safety consequences;
- RT2 has
  - medium likelihood and low financial consequences
  - Medium likelihood and high health & safety consequences.

Then for the RT1 the risk matrix is calculated as follows

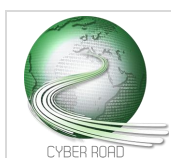
- financial risk of 20
- Health & Safety risk of 4

and for RT2 the risk matrix is calculated as follows

- financial risk of 10
- Health & Safety of 50

Research Topic	Financial Risk	Weighting factor	Health & safety Risk	Weighting factor
RT1	20		4	
RT2	10		50	

Then remains to assign the weighting factors and we consider two very extreme (and unrealistic cases): the weighting factor for financial risk is assumed 1.5 and for Health & Safety is assumed 2 then the overall risk is computed in the table below.



Research Topic	Financial Risk	Weighting factor financial	Health & safety Risk	Weighting factor H&S	Score
RT1	20	1.5	4	2	38
RT2	10	1.5	50	2	115

Results of this example makes Risk ranking RT1 followed by RT2.

This example shows the approach and the flexibility of the ranking operation: the final CyberROAD list can be ranked according to risks and tuned, by carefully selecting the weights, according to stakeholders needs.



### Cyber ROAD

Development of the Cybercrime and Cyber-  
terrorism Research Roadmap



European Commission  
Seventh Framework Programme

## Creation of roadmaps based on scenario analysis

Confidential internal document

Version 1.0 – March 13, 2015

Responsible: Fabio Roli (UNICA)

Contributors:

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



## Aim of this presentation - 1

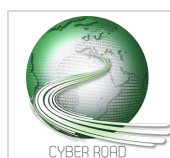


**This presentation, together with the companion document "Tutorial on Scenario Analysis and Roadmapping", is the sequel of the previous documents on the roadmapping methodology:**

- *D2.1 (Roadmapping Methodology and Guidelines for Information Collection and Assessment)*
- *Toward the CyberROAD roadmap, confidential internal document (slides, October 2014)*

**These slides aim at addressing the key issue #3 (*identifying candidate techniques for the creation of the roadmap*), specifying a complete methodology to develop *vertical*, exploratory roadmaps that will analyze possible future scenarios**

- *The methodology addresses the open issue "Which exploratory roadmap to do?" listed in the slides shared with the consortium in October 2014*





## Aim of this presentation - 2



These slides are also aimed at summarizing the proposed method for creation of research roadmaps based on

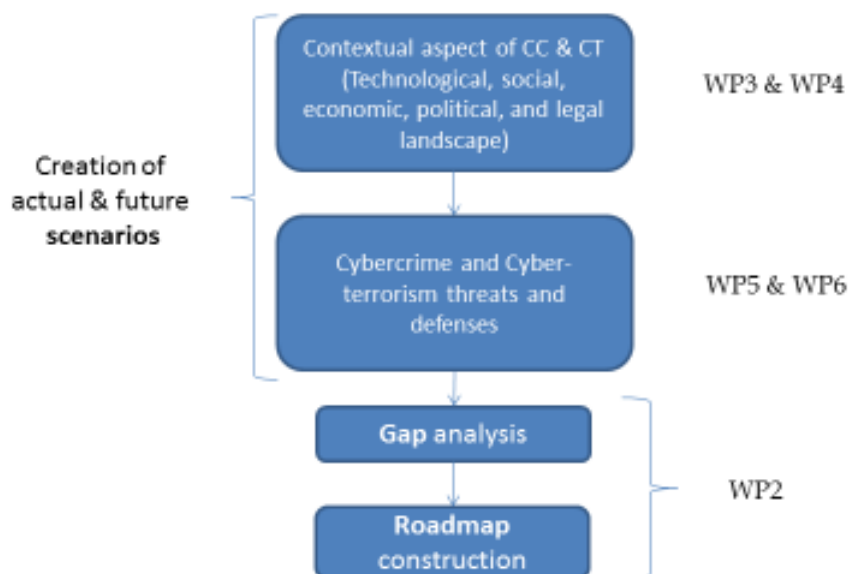
- *Scenario building*
- *Gap analysis*

More details can be found in the companion document "Tutorial on Scenario Analysis & Roadmapping"

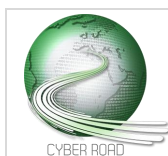
3



## Main steps of CyberROAD roadmapping



4





## Terminology - 1



- **STATE:** the whole set of technological, social, economic and political conditions that define the context of cybercrime (CC) and of cyber-terrorism (CT), and the corresponding specific threats and defenses, either in the present or in a hypothetical future
- **SCENARIO:** a concise and schematic representation of the state (actual or future), aimed at identifying “threats” and “defenses”
- **VERTICAL SUB-SCENARIO (VIEW):** the elements of a scenario concerning only a given subject, i.e. workforces, private transports, etc. For the sake of brevity, the term VIEW will also be used
- **THREAT:** any circumstance or event, not necessarily related to technology, with the potential to adversely impact either an information system or the society or group of people which makes use of and benefits from the services offered by that system
- **DEFENCE:** any mechanism, not necessarily technological (i.e., a policy, a legislative framework, and so on), with the potential to either stop or mitigate a threat, or to make its legal prosecution easier

5



## Terminology - 2



- **KEY DRIVERS:** the key driving factors that are expected to influence the development of future scenarios emerging from the current ones
- **RESEARCH GAP:** a mismatch between a research subject related to a specific threat/ defence in the actual state and in a future view. It emerges from the comparison between the current knowledge and future needs, i.e., from the **gap analysis**
- **GAP ANALYSIS:** the process of comparing actual and future views in order to identify research gaps
- **RESEARCH TOPIC:** a set of related research gaps
- **VERTICAL ROADMAP:** a collection of paths describing actions required to address a specific research topic and to reach a given objective in the future
- **ROADMAP:** the set of vertical roadmaps that will be developed to address the research topics identified in the Cyber ROAD project

6



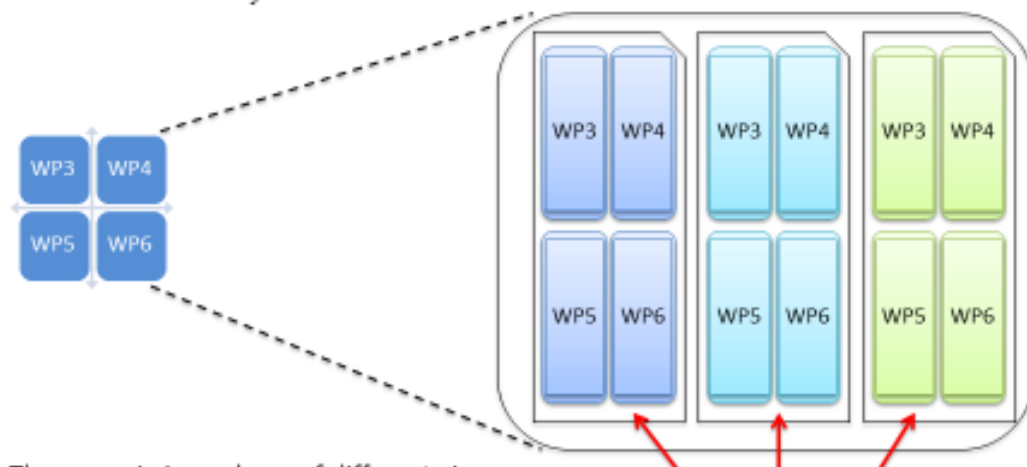




## Scenario



A concise description of the current or future state aimed at identifying *"threats"* and *"defenses"*



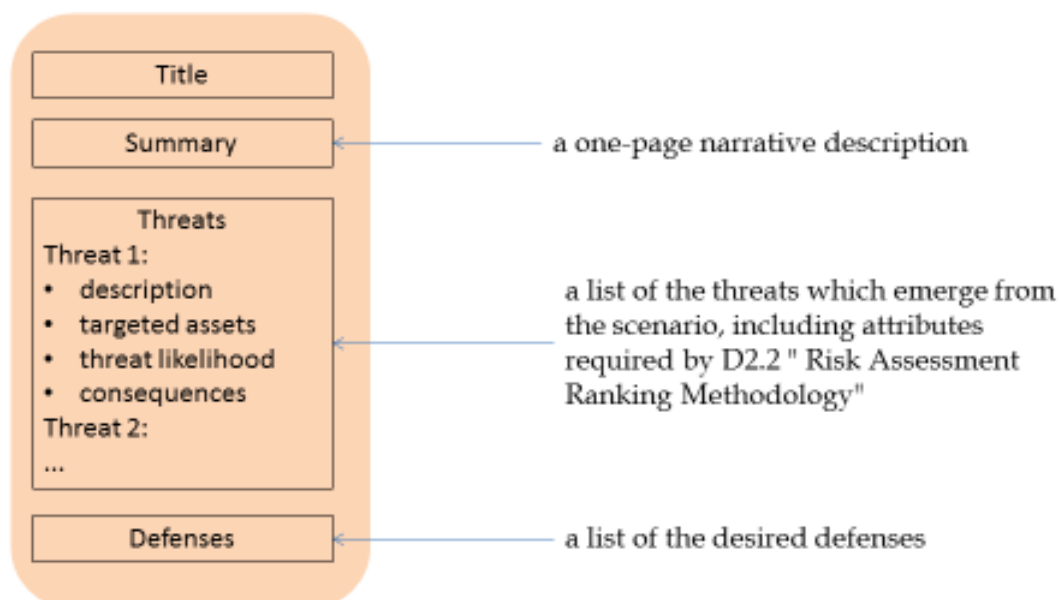
The scenario is made up of different views. WP3-WP6, under the coordination of WP2, contribute to define all the views.

Each **view** focuses on specific aspects of the scenario

7



## Scenario template



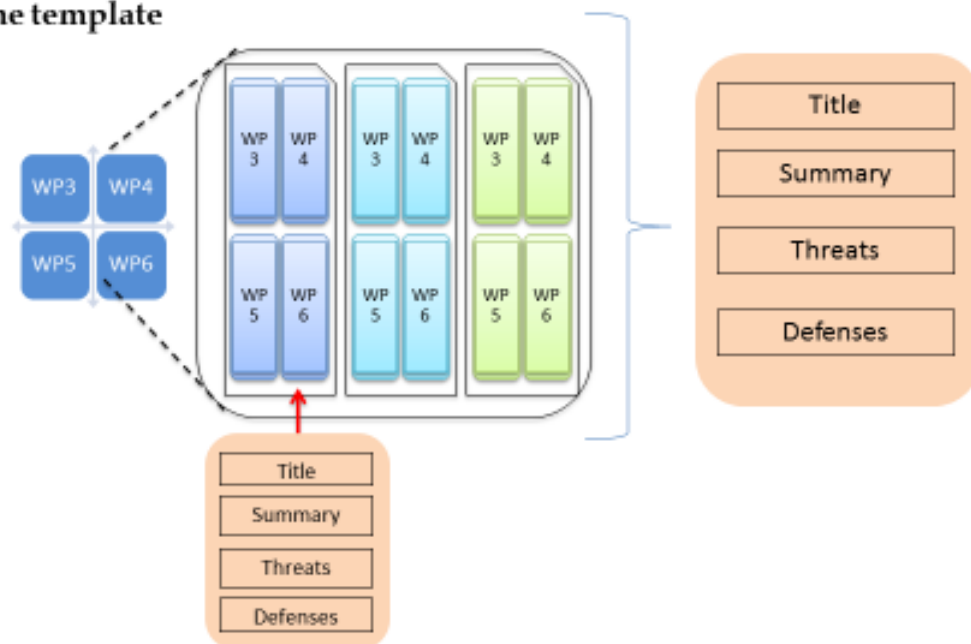
9



## Scenario



Both the entire scenario and every single view can be described using the same template



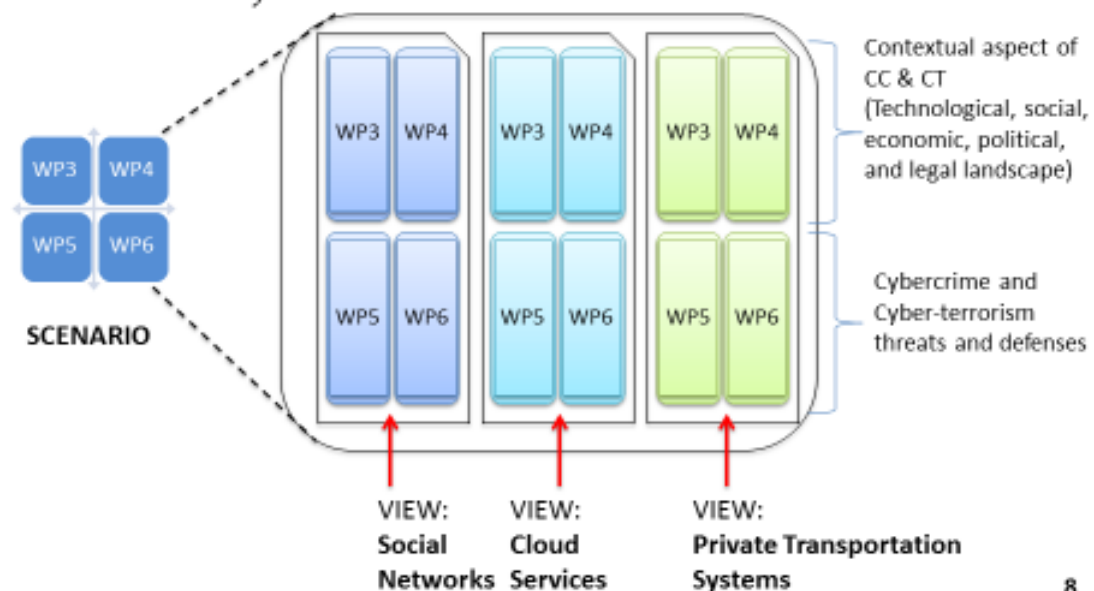
10



## Scenario



A concise description of the current or future state aimed at identifying *"threats"* and *"defenses"*



8

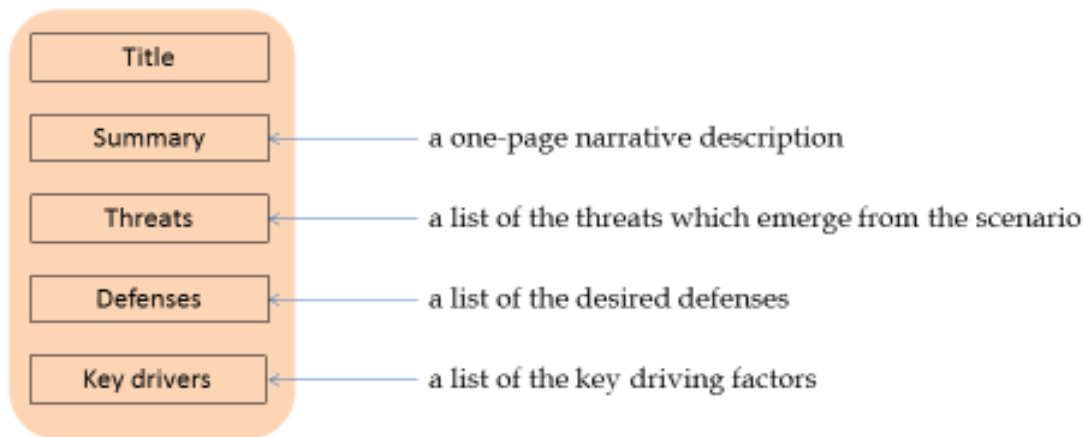




## Key drivers for current scenario



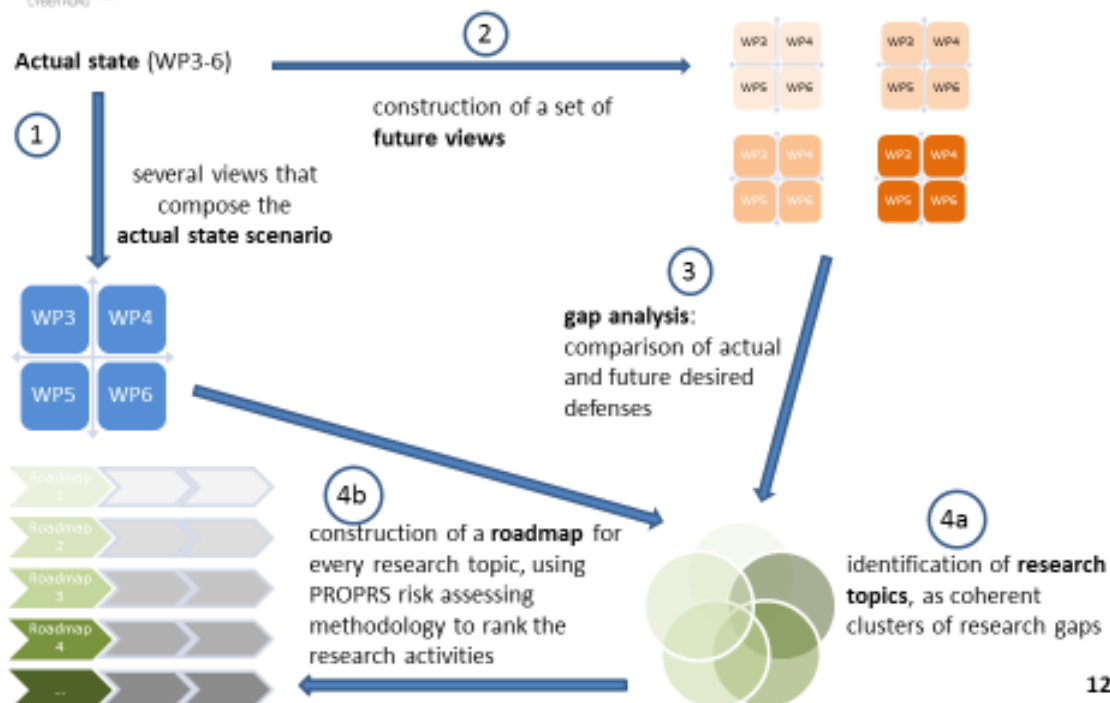
Template of current scenario may be enriched with a slot containing the key driving factors that are expected to influence the development of future scenarios emerging from the current one



11



## Roadmap creation based on scenario analysis

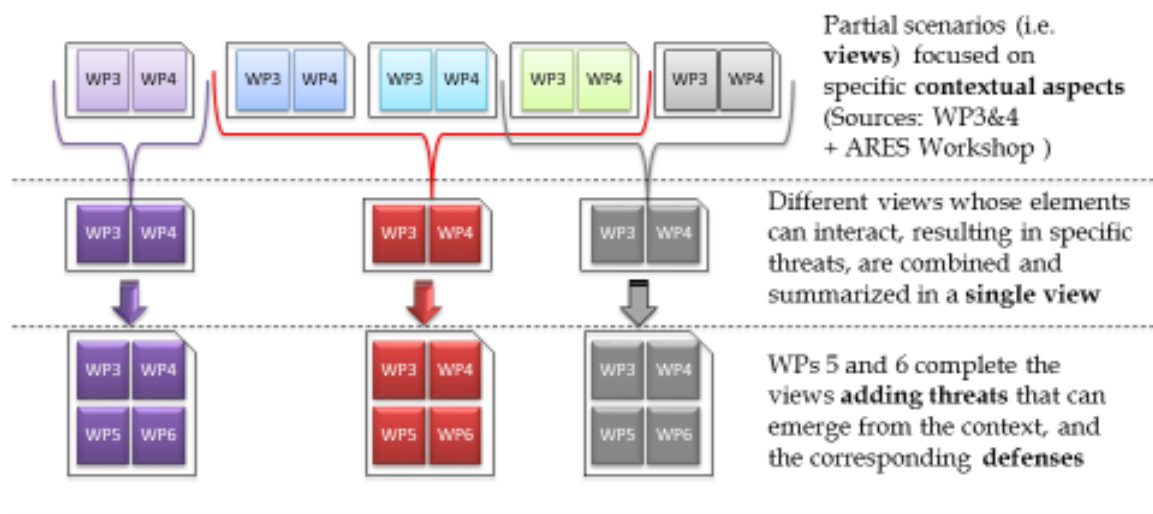


12

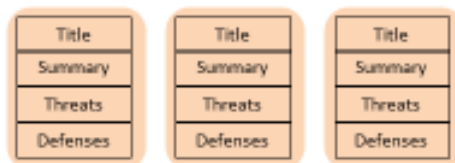




## How to build views



**GOALS:**



A set of views that describe the **actual** or the **future** scenarios

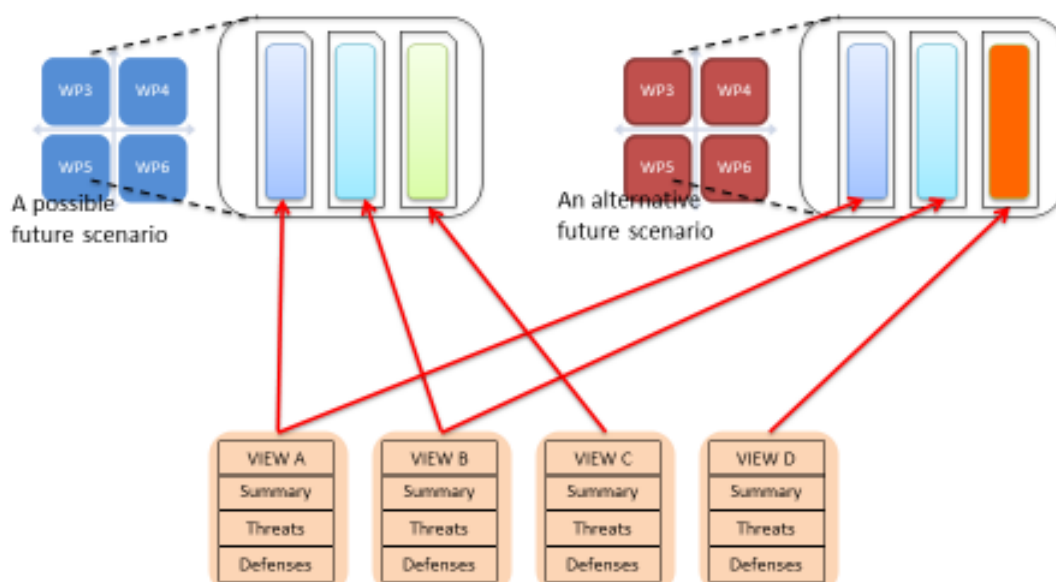
13



## Future scenarios



Different future views can contribute to depict future scenarios.  
Incompatible views (C and D in the example) define alternative scenarios.



14



# Gap analysis



## Set of actual views



## Set of future views



Gap  
analysis

Gaps



15



# Gap analysis – An example



## Set of actual views



threat

Malware delivered to the mobile devices through community based traffic and navigation apps distributed through non official marketplaces

defense

- Mobile anti malware software
- Network based Intrusion Detection Systems

## Set of future views



threat

Malware coming from the mobile devices connected to the car infotainment system is able to reach the Engine Control Unit through the CAN Bus, and, after bypassing the Security Access service, to access privileged functions on the vehicle

defense

Intrusion detection systems capable to identify anomalous traffic flowing through the CAN Bus

Gap  
analysis

Gap

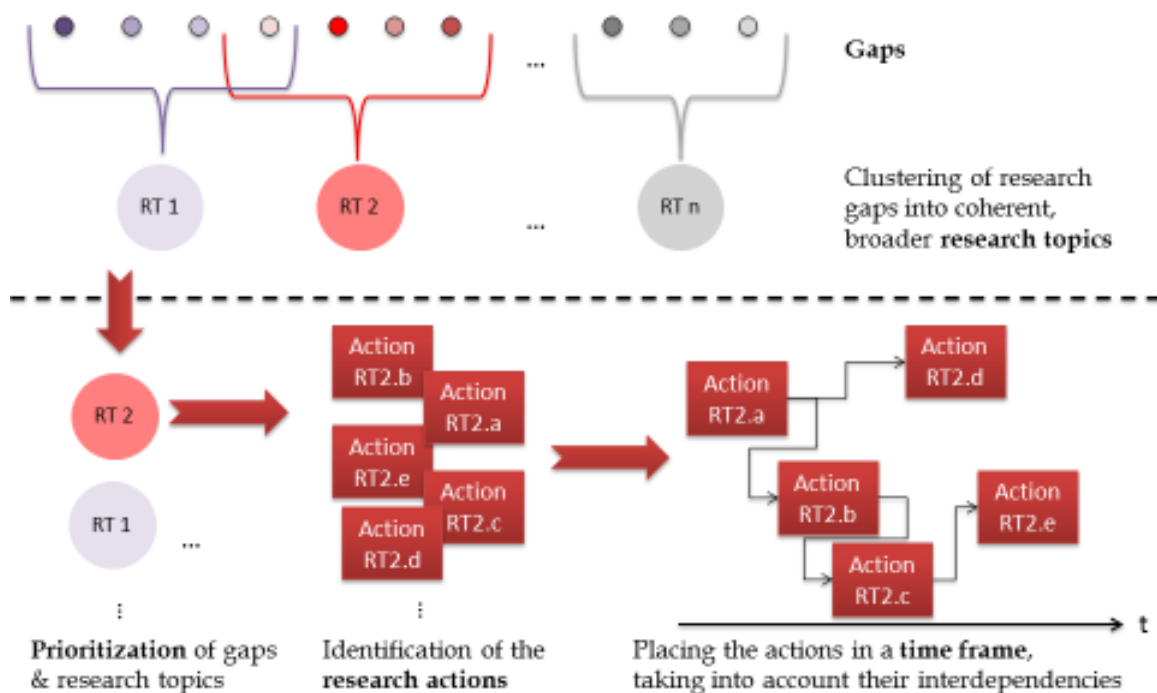
Even if anti-malware and intrusion detection solutions exist, none of them is available which is able to work on the CAN Bus; anomaly based solutions are sought for their capability to work against zero-days

16





# Roadmap construction



## What can be found in the companion document



The companion document "*Tutorial on Scenario Analysis & Roadmapping*" contains:

- a more detailed definition of "scenario"
- a template for describing scenarios
- how to implement the roadmapping methodology described in these slides
- Examples of
  - actual scenario
  - future views
  - gap analysis
  - construction of a vertical roadmap



- Codagnone, C. & Wimmer, M.A. (eds.). Roadmapping eGovernment Research: Visions and Measures towards Innovative Governments in 2020. MY Print snc di Guerinoni Marco & C, Clusone, 2007
- Geschka, H. & Hahnenwald, H., Scenario-Based Exploratory Technology Roadmaps - A Method for the Exploration of Technical Trends; in: Technology Roadmapping for Strategy and Innovation, Moehrle, M. G.; Isenmann, R. & Phaal, R. (Eds.), Springer Berlin Heidelberg, 2013, 123-136
- George Wright, Ron Bradfield, George Cairns, "Does the intuitive logics method - and its recent enhancements - produce "effective" scenarios?", Technological Forecasting & Social Change 80 (2013) 631-642
- Ron Bradfield, George Wright, George Burt, George Cairns, Kees Van Der Heijden, "The origins and evolution of scenario techniques in long range business planning", Futures 37 (2005) 795-812







Funded by the European Commission

Seventh Framework Programme



# CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

## Tutorial on Scenario Analysis & Roadmapping

April 23 rd, 2015

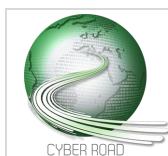
Start date of the Project: 1st June 2014.

Duration: 24 months

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

Version: 2.0

Project funded by the European Commission under the Seventh Framework 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)	✓



D2.2 Risk Assessment Ranking Methodology

Funded by the European Commission under the Seventh Framework Programme

Page 40 of 57



# Tutorial on Scenario Analysis & Roadmapping

**SUMMARY AND PURPOSE OF THIS DOCUMENT:** This internal document provides details to implement the roadmapping methodology outlined in the companion slides.

This document, together with the slides *“Creation of roadmaps based on scenario analysis”*, is a sequel of the previous documents on the roadmapping methodology:

- *D2.1 (Roadmapping Methodology and Guidelines for Information Collection and Assessment)*
- *Toward the CyberROAD roadmap*, confidential internal document (slides, October 2014)

It is aimed to address the key issue #3 (*identifying candidate techniques for the creation of the roadmap*), specifying a complete methodology to develop vertical, exploratory roadmaps that will analyze possible future scenarios.

The methodology addresses the open issue *“Which exploratory roadmap to do?”* listed in the slides shared with the consortium in October 2014.

Section 1 [Terminology] gives the definition of the terms used in this document.

The construction of the roadmap starts from the definition of the actual state of Cybercrime (CC) and Cyberterrorism (CT) and their contextual environment, which is the output of WPs 3-6 in deliverables D3.1, D3.2, D4.1, D4.2, D4.3, D4.4, D5.1, D6.1. The roadmapping methodology consists of (see slides 4 and 12):

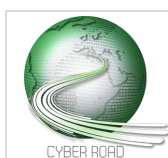
1. summarizing the actual state of CC and CT as a set of "vertical sub-scenarios" or "views",
2. envisioning possible future views of CC and CT,
3. performing a gap analysis by comparing the actual and future views,
4. clustering research gaps into coherent, broad research topics, and constructing a “vertical” roadmap for each topic;
5. defining a small set of future scenarios as coherent clusters of views.

This document also provides:

- templates for describing views, scenarios and the results of gap analysis;
- examples of actual and future views, of the outcome of gap analysis, and of a vertical roadmap.

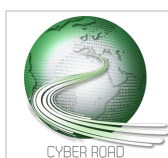
## Keywords:

State, Scenario, Roadmapping, Gap analysis, Research gap, Research topic, Research roadmap.



## TABLE OF CONTENTS

<b>1</b>	<b>TERMINOLOGY .....</b>	<b>43</b>
<b>2</b>	<b>SCENARIO BUILDING .....</b>	<b>44</b>
2.1	DEFINITION OF SCENARIO .....	44
2.2	SCENARIO TEMPLATE .....	44
<b>3</b>	<b>THE ROADMAPPING METHODOLOGY.....</b>	<b>46</b>
3.1	FIRST STEP: DEFINING THE ACTUAL STATE VIEWS (SLIDE 7-10) .....	46
3.2	SECOND STEP: ENVISIONING FUTURE VIEWS (SLIDE 13) .....	46
3.3	THIRD STEP: GAP ANALYSIS (SLIDE 15 AND 16) .....	47
3.4	FOURTH STEP: ROADMAP CONSTRUCTION (SLIDE 17) .....	47
<b>4</b>	<b>EXAMPLE OF ACTUAL STATE .....</b>	<b>48</b>
<b>5</b>	<b>EXAMPLE OF FUTURE VIEWS.....</b>	<b>49</b>
5.1	VIEW TITLE: PRIVATE TRANSPORTATION SYSTEMS .....	50
5.2	VIEW TITLE: SOCIAL NETWORKS .....	50
5.3	VIEW TITLE: CLOUD SERVICES .....	51
5.4	MERGING COHERENT VIEWS .....	51
<b>6</b>	<b>EXAMPLE OF GAP ANALYSIS.....</b>	<b>51</b>
<b>7</b>	<b>EXAMPLE OF ROADMAP CONSTRUCTION .....</b>	<b>54</b>
7.1	CLUSTERING OF RESEARCH GAPS INTO RESEARCH TOPICS.....	54
7.2	PRIORITIZATION OF THE RESEARCH TOPICS & GAPS.....	54
7.3	IDENTIFICATION OF THE RESEARCH ACTIONS .....	54
7.4	PUTTING THE ACTIONS IN A TIME FRAME AND CREATING VERTICAL EXPLORATORY ROADMAPS .....	56



# 1 TERMINOLOGY

**STATE:** the whole set of technological, social, economic and political conditions that define the context of cybercrime (CC) and of cyber-terrorism (CT), and the corresponding specific threats and defenses, either in the present or in a hypothetical future time.

**SCENARIO:** a concise and schematic representation of a state (actual or future), aimed at identifying threats and defenses.

**VERTICAL SUB-SCENARIO:** the elements of a scenario concerning only a given subject, i.e. workforces, private transports, etc. For the sake of brevity, the term VIEW will also be used, with a different meaning with respect to its use in relational data bases.

**THREAT:** any circumstance or event, not necessarily related to technology, with the potential to adversely impact either an Information System or the society or group of people which makes use of and benefits from the services offered by that system. It is also considered a threat whatever circumstance or condition makes it difficult to properly defend a system or to carry out the forensic activities aimed to investigate the event, to identify responsables, and/or eventually to prosecute them.

**DEFENSE:** any mechanism, not necessarily technological (i.e. a policy, a legislative framework, and so on), with the potential to either stop or mitigate a threat, or to make its prosecution easier.

**KEY DRIVERS:** the key driving factors that are expected to influence the development of future scenarios emerging from the current ones.

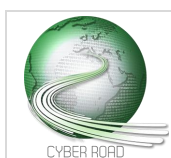
**RESEARCH GAP:** a mismatch between a research subject related to a specific threat/defense in the actual state and in a future view. It emerges from the comparison between the current knowledge and future needs, i.e. from the gap analysis.

**GAP ANALYSIS:** the process of comparing actual and future views in order to identify research gaps.

**RESEARCH TOPIC:** a set of related research gaps.

**VERTICAL ROADMAP:** a collection of paths describing actions required to address a specific research topic and to reach a given objective in the future.

**ROADMAP:** the set of vertical roadmaps that will be developed to address the research topics identified in the Cyber ROAD project.



## 2 SCENARIO BUILDING

### 2.1 DEFINITION OF SCENARIO

We propose to use the **scenario building** approach (widely used in exploratory roadmapping<sup>12</sup>) as the first step toward the construction of vertical, exploratory roadmaps.

In the context of CyberROAD, a scenario is a concise description of the current state of CC and CT and their contextual environment (namely, society, politics, economy and technology), or an internally consistent and coherent sketch of a possible future state (e.g., in 2020). A scenario can be made up of several vertical sub-scenarios, also called “views”, each focusing on a specific aspect of the current or future state (e.g., *Payment Systems*, *Driverless Vehicles*, *Mobile Devices and Services*). Both views and scenarios have to be represented with the template described in the following section.

Views are used to identify research gaps emerging from the comparison between the current state and the possible future states, which in turn will lead to the CyberROAD roadmap (see slide 15, 16 and 17). Scenarios are used at the end of the roadmapping process, in order to concisely represent some possible future state. Future scenarios are obtained by combining congruent views, while incompatible views give rise to alternative scenarios.

### 2.2 SCENARIO TEMPLATE

The template in Table 1 provides a guideline for describing the actual and future views and scenarios in a uniform way, and shows examples of the elements that can be addressed in a view or scenario. The number of elements addressed may change as a consequence of the scope of the view: a limited number of elements is addressed by small and focused views (e.g. a view on *Driverless Vehicles*), whereas larger views (e.g. a view on *Mobile Devices and Services*) may address a higher number of elements. CyberROAD partners are free to introduce additional elements and to deviate from the template, if it is deemed too restrictive. However, deviations should be clearly motivated.

Each view or scenario must be made up of:

- a **title** that summarizes its subject;
- a **summary**, in the form of a one-page narrative description;
- a list of the **threats** related to CC and CT which emerge from the view or scenario;
- a list of the corresponding desired **defenses**, including non-technical ones (e.g., legislative and economic countermeasures).

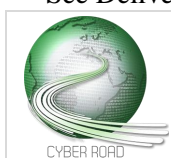
According to deliverable D2.2 "Risk Assessment Ranking Methodology", for each threat three attributes have to be specified beside its description: the assets targeted by the threat, the threat likelihood, and its consequences.

The template of current scenarios may be enriched with a slot containing the key driving factors that are expected to influence the development of future scenarios emerging from the current one.

Examples of an actual state scenario and of future views are provided in sections 4 and 5 respectively.

---

<sup>12</sup> See Deliverable D2.1, and [http://scenariothinking.org/wiki/index.php/What\\_is\\_Scenario\\_Thinking?](http://scenariothinking.org/wiki/index.php/What_is_Scenario_Thinking?)



Scenario/ Vertical Sub-Scenario (View)		
<p><b>Summary:</b> ... (one page).</p> <p>A list of the possible elements that can be addressed is provided below here, as an example. CyberROAD partners are free to introduce additional elements.</p> <p><b>Contextual environment</b> (gathers WP3 outcomes)</p> <ul style="list-style-type: none"> <li>• Society (e.g. how the society look like, role of individuals and communities, internet governance, identity management)</li> <li>• Political system and climate (e.g. societal and democratic values, governance value, transparency, security, enforcement, compliance, political system)</li> <li>• Economic climate (e.g. employment, type of labour, age composition labour force, position in the world, ubiquitous workforces, use of virtual currencies, personal data selling business models)</li> <li>• Legal and Law enforcement issues (skills of the law enforcement, jurisdiction, (personal) data protection and liability, right to be forgotten, intellectual property)</li> </ul> <p><b>Technology &amp; (technology enabled) services</b> (gathers WP4 outcomes)</p> <ul style="list-style-type: none"> <li>• ICT available: which kind of technology will we be using in 2020? <ul style="list-style-type: none"> <li>i. Payment systems</li> <li>ii. Mobile devices</li> <li>iii. IoT</li> <li>iv. Sensors &amp; wearables</li> <li>v. Driverless vehicles</li> <li>vi. Augmented reality</li> <li>vii. Remote presence</li> <li>viii. Web 3.0</li> </ul> </li> <li>• Services: which kind of services will we be using in 2020? How the current services will evolve in the next 5 years? <ul style="list-style-type: none"> <li>i. Communication service providers</li> <li>ii. Content service providers</li> <li>iii. Cloud service providers</li> <li>iv. Reputation and cyber risk management/insurances</li> </ul> </li> </ul> <p><b>Cybercrime &amp; Cyberterrorism specific issues</b> (gathers WP5 and WP6 outcomes)</p> <ul style="list-style-type: none"> <li>• Offensive technologies (malware evolution, spam generation, social engineering, )</li> <li>• Defensive technologies (intrusion &amp; malware detection, spam filtering, ...)</li> <li>• Programming techniques &amp; ARM coding</li> <li>• Business models, Marketplace blackmarkets, Targets</li> </ul> <p><b>Possible key driving factors</b> (only for current scenarios)</p>		
Threats		Desirable countermeasures
Threat 1	Threat description	Desirable countermeasures for threat 1
	Assets targeted by the threat	
	Threat likelihood	
	Consequences of the threat	
...	...	...

**Table 10. Template for representing Scenarios and Vertical Sub-Scenarios (i.e. Views)**

## 3 THE ROADMAPPING METHODOLOGY

### 3.1 FIRST STEP: DEFINING THE ACTUAL STATE VIEWS (SLIDE 7-10)

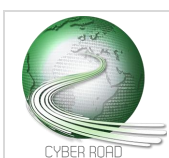
The actual state of CC and CT and of their contextual environment, defined in WPs 3-6, has to be summarized according to the template in section 2. The actual state is made up of a title, a one-page summary, and a list of threats and of the corresponding available defenses. CyberROAD partners may also consider to split the whole actual state in two smaller ones, one focusing on CC and the other focusing on CT, to better focus on the respective threats and defenses.

### 3.2 SECOND STEP: ENVISIONING FUTURE VIEWS (SLIDE 13)

The goal of this step is to produce a set of possible **views** of the **future**, which should explore a range of potential evolutions of CC and CT and of their contextual environment as wide as possible, highlighting the emerging **threats** and the **desirable defenses**.

This can be attained with three sub-steps (slide 13):

- a) WPs 3 and 4 build **initial views** focused on specific contextual aspects of CC and CT, related to one or more of the domains investigated by these WPs (society, politics, economy and technology). Each partner can focus on its own domain of expertise. Partners working also in WP5 and/or WP6 can add to their views specific aspects of CC and CT, envisioning the possible, corresponding threats and defining the desired defenses. Works submitted to the ARES Workshop can also be exploited to integrate the set of views produced by the CyberROAD partners. Each view must be described according to the template of section 2: a title, a one-page summary, and (if already defined) a list of threats and defenses.
- b) WPs 3 and 4 cluster related initial views to obtain the **final views** (which at this step will contain aspects related mainly to the contextual environment of CC and CT). It is up to the CyberROAD partners to identify the most relevant and interesting clusters of initial views, among all the possible ones, according to the above mentioned goal of exploring a range of potential evolutions of CC and CT and of their contextual environment as wide as possible. The following criteria are also suggested:
  - A final view can be obtained by merging initial views that are **coherent** (non-contradictory), and contain elements which can **interact**, resulting in specific threats. For instance, the strongly related views on *Social Networks* and *Cloud Services* depicted in section 5 can be merged to build a larger view on *Personal Data Management*.
  - A given initial view can be included into **more than one** final view. For instance, this can happen when a view A is related to two other views B and C, whereas B and C are contradictory or their combination does not permit to envision new threats: in this case one final view can include A and B, and another one A and C.
- c) WPs 5 and 6 complete the final views produced in step b) by adding the specific aspects related to CC and CT, i.e., by envisioning the possible, corresponding threats and defining the desired defenses. Some of or all the initial views that compose a final view may already include threats and defenses; if so, since such threats and defenses were independently defined for each initial view in step a), they should be revised and integrated (if needed) in light of the union of such initial views.



Each final view must be described according to the template of section 2.

### 3.3 THIRD STEP: GAP ANALYSIS (SLIDE 15 AND 16)

The goal of this step is to identify the research gaps that emerge from the comparison of each of the future views with the actual state. A research gap is defined as a specific research issue to be addressed to enable a given defense.

The research gaps must be identified comparing the desired defenses in the depicted future with the actual defense and the body of knowledge related to the desired defense.

To this aim, for each future view the threats<sup>13</sup> and the corresponding desired defenses must be compared with those available in the actual state. This comparison must be summarized in a table (see the example in Table 2), in which each row contains one threat (either known or novel), the desired defense existing/pursued in the actual state (only for known threats), the desired defense in the future view, and the identified research gaps.

Scenario title			
Threat	Defense (actual state)	Defense (future view)	Research gaps
Threat #1	Defense #1	Defense #1	Research gap #1
	Defense #2		Research gap #2
Threat #2	Defense #3	Defense #2	Research gap #3
		Defense #3	Research gap #4
		Defense #4	

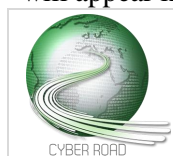
Table 11. Template for the Gap Analysis

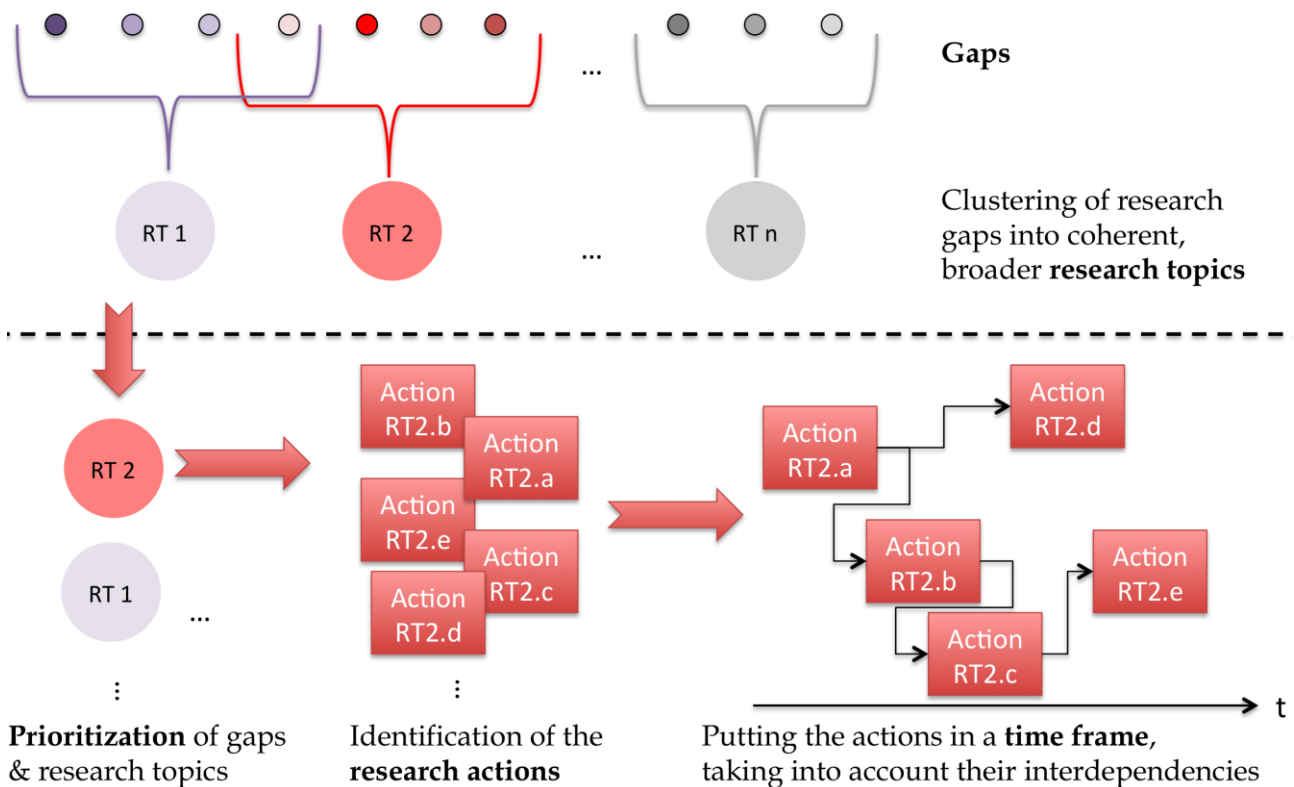
### 3.4 FOURTH STEP: ROADMAP CONSTRUCTION (SLIDE 17)

Once the research gaps have been identified, the last step will lead to the construction of the CyberROAD roadmap. This will be attained by two sub-steps (Figure 1):

- Defining a set of broad research topics, as **coherent clusters of related research gaps** emerging from one or more actual/future views, and prioritizing them using the risk assessment methodology defined by PROPRS (Task 2.2), taking into account the relevance of the threats they address.
- Constructing a roadmap for each research topic (vertical roadmap). This is attained by prioritizing the corresponding research gaps using the same methodology mentioned above, identifying the specific research actions required to address such gaps, and putting the actions into a clear time frame, taking into account their interdependencies.

<sup>13</sup> Threats that already exist in the actual state and that are foreseen to be not solved in the future views, shall be included in the gap analysis as well, together with the new threats that do not exist in the actual state and will appear in the future view only.





**Figure 13. The roadmap construction process.**

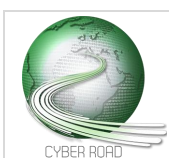
## 4 EXAMPLE OF ACTUAL STATE

This section provides a simple example of the actual state, described according to the template of section 2.

### SUMMARY:

The definition of social culture has changed with the social networking revolution, and the modern society is now a place where physical and virtual encounters seamlessly merge, even if a strong asymmetry persists in the way people do perceive the concept of “reputation” in their real and digital lives. The process of developing inter-personal relationships has become easier through social web sites. Recent developments in social networking have transformed the world from a social perspective; however, this new type of socializing has raised concerns about the privacy and security of Internet users. Mobile terminals played a key role in the growth of social networks. Thanks to mobile and ubiquitous terminals, users can in fact access their profiles as well as services that allow them to complete a task in any possible place, home, public spaces or company office. All these opportunities create a blending between private and professional lives due to the flexibility to work at any time from different locations.

There is not full trust neither on social platforms nor on cloud services, especially because the terms of service and the legislation on privacy and data protection are severely lacking. Nevertheless, users want to use those services and are therefore willing to give away personal data, following a data-for-(free) services logic, with machines collecting personal data from users who want to have access to services. Moreover, many different services and social networks do exist and users commonly have an account on several of them. Each service is fairly isolated from the others and this makes challenging for the users to carefully manage their identities and data, which are then heavily exposed especially to phishing attacks aimed to steal users’ credentials. Many services use two-factors authentication mechanisms as a countermeasure against these attacks. Emails are still a valid vehicle to deliver both phishing and malware, but fake social networks profiles are also used. The absence of a score to measure reputation and security of websites makes companies paying little to no attention on the security of their websites, that can be often easily





compromised with automatic tools and then used to deliver malware. Anti-spam filters and anti-malware solutions are quite effective against large campaigns but can definitely do less against targeted and well-crafted attacks. Attacks target not only private users but also companies, which look with great interest at the cloud based solutions & services, mainly because cloud technologies enable more flexible work paradigms and an overall reduction of costs, which is a relevant aspect in a context of global recession.

Cloud and social platform are accessed not only through the traditional platforms (PCs, mobile), but also through a number of wearable devices (e.g. watches) whose market is rapidly growing. More in general, the availability on the market of powerful hardware (CPUs, sensors, transmitters) at very low prices is enabling a number of different applications, especially in the areas of Home Automation and e-Health. Transportation systems are also benefitting from these advancements. UAV are available on the market at very low prices and become to be used in business applications. Research on self-driving cars is still ongoing, and yet they are used nowhere in the world, mainly for technological limitations but also in consequence of the fact that the required regulations have been not put in place. Nevertheless, some countries are running pilot projects and are building some of the required infrastructures, in particular wireless sensor networks. Cars rented through sharing services only represent a negligible fraction of those circulating in European streets, and people mainly drive their own car. Billing mechanisms for rented cars are based on traditional models where costs are calculated on the length of the rent period and on the mileage. Local authorities deliver informations and messages to the users primarily using displays installed along the roads. In addition, after the widespread use of mobile technologies a number of community-based traffic and navigation apps have been developed which let drivers to share informations about the traffic in real time.

#### **Threats:**

- Malware delivered to the mobile devices through community based traffic and navigation apps distributed through non-official marketplaces
- Phishing attacks to steal users' credentials
- Malicious profiles used to distribute malware
- Social Engineering and Targeted Attacks
- Ransomware
- The absence of supranational regulations makes hard for the law enforcement agencies to get access to the users' data stored in the cloud and get access to social networks profiles in case of crime. This severely limits their capability to prosecute certain categories of crime.

#### **Available countermeasures:**

- Mobile anti-malware software
- Network based Intrusion Detection Systems
- Anti-spam filters
- Safe browsing solutions integrated in the web browser
- Two-factors authentication
- Users' profiling based on usage patterns (e.g., geolocalisation)
- Cryptography used to encrypt data stored in the cloud
- Anti-malware solutions for both desktop and mobile platforms

## **5 EXAMPLE OF FUTURE VIEWS**

This section provides a simple example of a set of possible future views, described according to the template of section 2.

## 5.1 VIEW TITLE: PRIVATE TRANSPORTATION SYSTEMS

### SUMMARY:

Widespread use of automatic transports (e.g., electric cars), all of which implies the following aspects:

- Web application in user's mobile device that knows daily movements. Both the presence and destination are stored in the mobile device
- Latest news and additional information from local authorities and from pervasive wireless sensor networks are shown on the display, which is invisibly integrated into the windshield. Local authorities can alter markers to facilitate smoothly running traffic, avoid jams, and achieve an equal load on the roads.
- Such infrastructure is also open to private advertisements (in order to amortize the costs)
- Monthly transport is calculated by an app in on the user's mobile phone, which automatically connects to the car, enables the user to use it and exchanges data about the duration of the voyage.

Only the mileage is recorded and the built-in privacy extensions hinder a linkup to geolocation data.

### Threats:

- Rogue local authorities and wireless sensors deliver spoofed messages to the vehicles windshield to hijack vehicles flows and to produce heavy load on certain roads.
- Malware coming from the mobile device connected to the car infotainment system is able to reach the Engine Control Unit through the CAN Bus, and, after bypassing the Security Access service, to access privileged functions on the vehicle.

### Desired countermeasures:

- Authentication mechanisms are implemented through the Wireless Sensor Network, that prevent non-authorized nodes to connect to the network and to send messages.
- Intrusion detection systems able to identify anomalous traffic flowing through the CAN Bus.

## 5.2 VIEW TITLE: SOCIAL NETWORKS

### SUMMARY:

Social networks have evolved into communities of people who interact and exchange information in order to improve their lives and meet their needs, and evolving in terms of knowledge, skills, contacts,. This is facilitated by the fact that the trend is oriented to more decentralized networks, where there is no need any more to be member of the same social network to share the information with one's own friends. Event streams are transferred between social networks. Smart technologies, wearable electronics and IoT enable new methods to authenticate users, and in particular methods based on users' behaviour.

### Threats:

- Behaviour theft (like nowadays the identity theft)
- The absence of supranational regulations makes it hard for the law enforcement agencies to get access to the users' data in case of crime. This severely limits their capability to prosecute certain categories of crime.



#### Desired countermeasures:

- Situational security authentication system (based on behaviour of humans and machines)

### 5.3 VIEW TITLE: CLOUD SERVICES

#### SUMMARY:

User wants to complete a task in any possible place, home, public spaces or company office and over any possible device. The availability of large and long bandwidth through the whole Europe makes such services available to more than 90% of the EU citizens. EU is now moving toward a complete dematerialization of the personal dataspace on cloud services, which is seen as a strategic goal toward the achievement of the Digital Agenda objectives. Federated cloud now represent a common standard for both hardware and software companies. Repositories of social and transactional data, collectively known as the “digital commons”, exist. Purchasing habits, media consumption, and travel plans are all retrievable on these commons. Users’ privacy is totally preserved, since data are completely anonymized before being stored in the repository. Every user has a full control of his own dataspace and has also the possibility to sell his own data directly to the marketing companies, obtaining a revenue paid on a monthly basis by the buying company.

#### Threats:

- Behaviour theft (like nowadays the identity theft)
- Cross-border legal problems with cyber entities complying with laws frameworks of a foreign country.
- The absence of supranational regulations makes hard for the law enforcement agencies to get access to the users’ data stored in the cloud in case of crime. This severely limits their capability to prosecute certain categories of crime.
- Ransomware

#### Desired countermeasures:

- Situational security authentication system (based on behaviour of humans and machines)


### 5.4 MERGING COHERENT VIEWS

The two views on *Social Networks* and *Cloud Services* are not contradictory and are complementary. They can be merged in broader view on “Personal Data Management”. Threats and defenses should be revised and integrated (if needed) in light of the union of the initial views. New threats may also emerge as a result of this fusion.

## 6 EXAMPLE OF GAP ANALYSIS

This section provides a simple example of gap analysis, obtained from the comparison of the actual and future views above. The same (or very similar) gaps may emerge from the comparison of similar threats depicted by different views. All the views from which a gap emerged should be listed under the column Views. All the corresponding Threats and sought Defenses should be listed under the columns Threats and Defenses (future view).

In order to simplify referencing during the preparation of the roadmap, gaps must be also numbered and provided with a title.

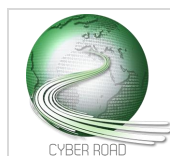
GAP #	Views	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
	D2.2 Risk Assessment Ranking Methodology				
	Funded by the European Commission under the Seventh Framework Programme				
	Page 51 of 57				

1	Transportation Systems	Malware coming from the mobile device connected to the car infotainment system is able to reach the Engine Control Unit through the CAN Bus, and, after bypassing the Security Access service, to access privileged functions on the vehicle.	<ul style="list-style-type: none"> <li>- Mobile anti-malware software</li> <li>- Network based Intrusion Detection Systems</li> </ul>	Intrusion detection systems able to identify anomalous traffic flowing through the CAN Bus.	Malware detection in unconventional environments
2	Transportation Systems	Rogue local authorities and wireless sensors deliver spoofed messages to the vehicles windshield to hijack vehicles flows and to produce heavy load in certain roads.	No countermeasure is available at present.	Source authentication and message integrity mechanisms are implemented through the Wireless Sensor Network that prevent non authorized nodes to connect to the network and to send messages.	Authentication in Wireless Sensor Networks
3	Social Networks	Behaviour theft	Users' profiling based on usage patterns (e.g. geolocalisation)	Situational security authentication system (based on behaviour of humans and machines)	Complex profiles monitoring
4	Cloud Services	Cross-border legal problems with cyber entities complying with legal frameworks of a foreign country.	No countermeasure is available at present.	EU Member States developed a coherent legal framework with 3 different levels of compliance, each one guaranteeing the possibility to operate in a certain number of EU countries.	Pan-European compliance
5	Cloud Services	The absence of supranational regulations makes it hard for the law	EU law enforcement has access only to	An EU authority is established which is	Protection of the citizens' privacy



		enforcement agencies to get access to the users' data stored in the cloud in case of crime. This severely limits their capability to prosecute certain categories of crime.	data stored within the borders of their own countries. Only for crimes related to child sexual abuse coordination with EUROPOL allows to bypass such limitation.	responsible for the prosecution of crimes related to child sexual abuse and crimes against the EU strategic interests and infrastructures. The authority is granted by law permanent access to the cloud services, which makes the prosecution of criminals faster and effective.	
--	--	---	--	---	--

GAP #	GAP Title	Description
1	Malware detection in unconventional environments	Even if anti-malware and intrusion detection solutions exists, none of them is available which is able to work on the CAN Bus. Anomaly based solutions are sought for their capability to work against zero-days.
2	Authentication in Wireless Sensor Networks	Sensor nodes are resource constrained, which severely limits the service quality of broadcast authentication while public-key based broadcast authentication schemes are used.
3	Complex profiles monitoring	Baseline technologies exists which allow to monitor both machines behavior (e.g. resource consumption) and users' behavior (e.g. geolocalisation), but effective frameworks to build complex profiles (user + machine) are still not available.
4	Pan-European compliance	Companies duties are specified at national level, which makes the current regulations extremely fragmented and poorly aligned.



5	Protection of the citizens privacy	The activity of the authority is in contrast with the Code of EU online right, since the users' right to privacy, which has to be considered as a fundamental right, is systematically infringed.
---	------------------------------------	---

## 7 EXAMPLE OF ROADMAP CONSTRUCTION

This section provides a simple example of roadmap construction, based on the above gap analysis.

### 7.1 CLUSTERING OF RESEARCH GAPS INTO RESEARCH TOPICS

As a further step toward the preparation of the roadmap, research gaps emerged from the gap analysis have to be grouped in coherent research topics. To devise criteria for such a grouping will be responsibility of the CyberROAD partners involved in Task 2.4 "Cyber security research roadmap generation". Each research topic has to be described according to the template of section 7.3, comprising a **title**, the **set of encompassed research gaps**, an **abstract**, and the suggested **research actions** to address the topic.

The identified research topics will be then passed for prioritization to the Risk Assessment Ranking Methodology developed by PROPRS in D2.2. Using the same methodology, priorities can be also assigned to the research actions within every single research topic.

As an example, the research gaps identified in section 6 can be grouped under the following two topics:

1. **Research Topic: *Developing a Pan-European legal framework***
  - **GAP #4** – Pan-European compliance
  - **GAP #5** - Protection of the citizens privacy
2. **Research Topic: *Security of complex and unconventional systems***
  - **GAP #1** - Malware detection in unconventional environments
  - **GAP #2** - Authentication in Wireless Sensor Networks
  - **GAP #3** - Complex profiles monitoring

### 7.2 PRIORITIZATION OF THE RESEARCH TOPICS & ACTIONS

Prioritization of the research topics shall be made according to the Risk Assessment Ranking Methodology developed by PROPRS in D2.2.

Within each topic, priorities will be assigned to the research actions and will be used, as described in section 7.4, to build the vertical exploratory roadmaps.

This document is not intended to provide an example of prioritization. CyberROAD partners should refer to D2.2 for details on the prioritization methodology.

### 7.3 IDENTIFICATION OF THE RESEARCH ACTIONS

The research topics must be described using the following format:

- The **title** and **number** of the research topic
- List of the encompassed research gaps:
  - gap **number** and **title**
- An **abstract** which concisely describes the research topic
- The **actions** to be taken to address the research topic; each action must be characterized in terms of:

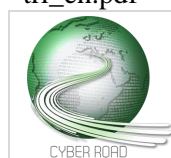
- **questions** to answer through the research activity
- a **time span** for addressing the research action
- the **actors** that have to implement these actions
- **information required to rank the research action**, according to D2.2 "Risk Assessment Ranking Methodology":
  - **distance to the market**, defined in terms of the Technology Readiness Level (TRL)<sup>14</sup>
  - **cost of the gap** relative to others, estimated in terms of the number of projects the EU should fund for getting proper results; to this aim, two kinds of FP7 projects can be considered as unit of measurement:
    - Small or Medium Scale focused research project (STREP): typical duration 18-36 months, 6-15 participants, EU contribution 1-4 M€, with an average around 2 M€
    - Integrated Project (IP): typical duration 36-60 months, 10-40 participants, total EU contribution 4-25 M€, with an average around 10 M€
  - **availability of competences in Europe**, which can be evaluated using a scale from 1 (minimum) to 5 (maximum)

As an example, the research topic ***Security of complex and unconventional systems*** depicted in Section 7.1 could be described as follows:

Research Topic #2	Title: <b><i>Security of complex and unconventional systems</i></b>
Encompassed research gaps	GAP #1 - Malware detection in unconventional environments  GAP #2 - Authentication in Wireless Sensor Networks  GAP #3 - Complex profiles monitoring
Abstract	To develop and enhance defense and protection mechanisms, developing defense mechanisms suitable for unconventional platforms (neither PC or mobile) and introducing disruptive paradigms to protect users from traditional threats.
Research Action #2.a	Are the hardware platforms for embedded system suitable to run anti-malware solutions? <ul style="list-style-type: none"> <li>• Do they have the required computational power?</li> <li>• What is the impact of an anti-malware solution on the energy consumption?</li> </ul>
	<b><u>Ranking information</u></b> <b>Distance to the market:</b> 5 <b>Cost of the topic:</b> 3 STREPs + 1 IP <b>Availability of competences in Europe:</b> 4
	<b>Time span for addressing the action:</b> 18 Months
	<b>Actors:</b> Research institutions, Industry
Research Action #2.b	Using biometric technologies to model users' behavior. <ul style="list-style-type: none"> <li>• What is their degree of maturity?</li> <li>• Will wearable sensors be able to provide information useful to model users' behavior?</li> </ul>
	<b><u>Ranking information</u></b>

<sup>14</sup> See the definition of TRL proposed by the European Commission in the Horizon 2020 context:

[http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014\\_2015/annexes/h2020-wp1415-annex-g-trl\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf)



	<b>Distance to the market:</b> 7 <b>Cost of the topic:</b> 4 STREPs + 2 IP <b>Availability of competences in Europe:</b> 5
	<b>Time span for addressing the action:</b> 24 Months
	<b>Actors:</b> Research institutions, Industry
Research Action #2.c	Do lightweight algorithms exist, capable to correlate information coming from different sources and to detect anomalies?
	<b>Ranking information</b> <b>Distance to the market:</b> 4 <b>Cost of the topic:</b> 4 STREPs + 1 IP <b>Availability of competences in Europe:</b> 4
	<b>Time span for addressing the action:</b> 30 Months
	<b>Actors:</b> Research institutions
Research Action #2.d	<ul style="list-style-type: none"> <li>• Are there technologies, available on the market and alternative to those currently used, which can allow to sense information useful for the detection of threats?</li> <li>• Shall the traditional architecture of computers and operating systems be drastically revised to make possible the introduction of alternative and more reliable protection systems?</li> <li>• Shall the EC regulations be changed to ensure the trustworthiness of hardware and software components?</li> </ul>
	<b>Ranking information</b> <b>Distance to the market:</b> 2 <b>Cost of the topic:</b> 8 STREPs <b>Availability of competences in Europe:</b> 3
	<b>Actors:</b> Research institutions, Industry, Policy-makers
	<b>Time span for addressing the action:</b> 18 Months

#### 7.4 PUTTING THE ACTIONS IN A TIME FRAME AND CREATING VERTICAL EXPLORATORY ROADMAPS

The two final steps toward the preparation of vertical, exploratory roadmaps are:

- To organize, in the time span from 2016 till 2020, the research actions in a roadmap, according to the inter-dependencies among the actions and the priorities of the research gaps that the actions address;
- To represent such a roadmap with a graphical sketch. An example of the final roadmap is provided in Figure 2 for the topic “*Security of complex and unconventional systems*”.





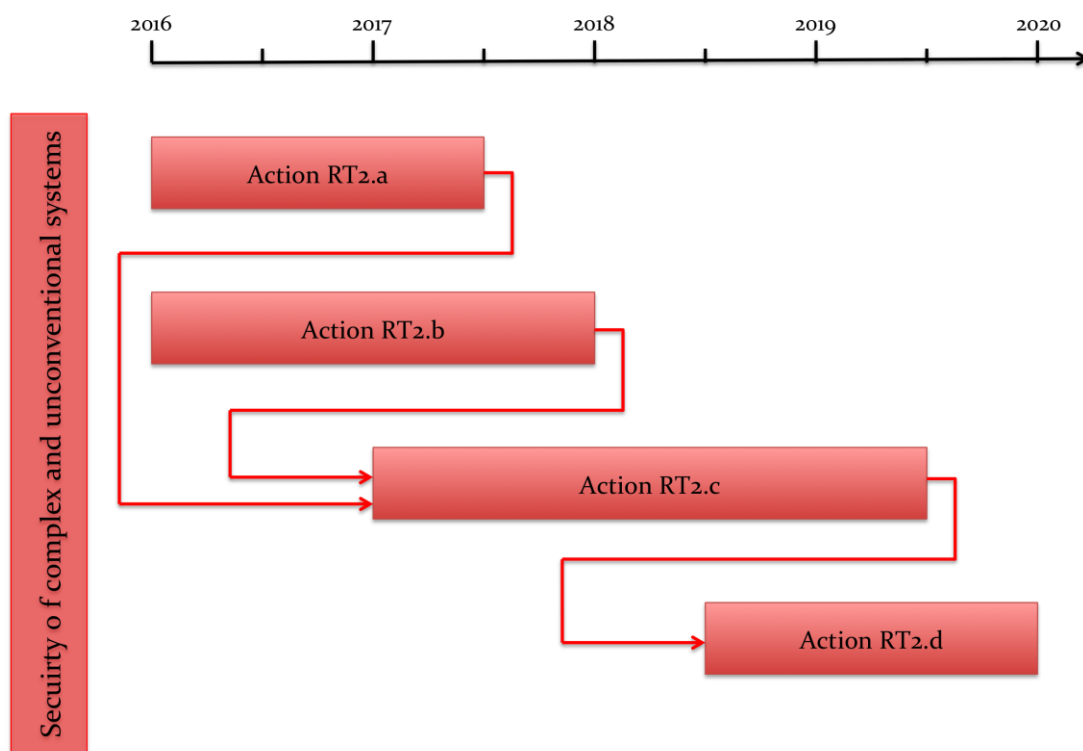


Figure 14. The research roadmap (2016-2020) for the topic "Security of complex and unconventional systems".