CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D7.7 - TUD Workshop Report

Date of deliverable: 30/06/2015
Actual submission date: 21/09/2015

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)	

Revision history

Version	Object	Date	Author(s)
0.1	Creation	29/06/2015	TUD
0.2	Revision	20/07/2015	TUD, NCSRD
0.2.1	Revision	20/07/2015	TUD, NCSRD
0.3	Revison	01/08/2015	TUD, NCSRD
0.4	Revision	01/09/2015	TUD, NCRSD
0.7	Revision	04/09/2015	TUD
0.9	Post Review and additions	16/09/2015	TUD, NCSRD, UNICA
1.0	Final for submission	21/09/2015	TUD

D7.7
TUD Workshop Report

Responsible
Erik Tews (TUD),
André Schaller (TUD).

Contributor(s)
Erik Tews (TUD),
Christian Schlehuber (TUD),
Olga Segou (NCSRD).

Summary: The CyberROAD project has been funded under the 7th Framework Programme in order to provide insight on current and future Cyber Crime and Cyber Terrorism research. CyberROAD aims to develop a comprehensive research roadmap, which will enumerate current research gaps and anticipate emerging threats.

CyberROAD devotes Work Package 7 to high-impact dissemination and exploitation activities. This document (D7.7 "First Year Workshop Report") presents the workshop activities that were undertaken by the consortium. Workshop activities were necessary for the effective dissemination and exploitation of key CyberROAD results and the request of feedback from professional communities and the general public, as performed within the project's first year of activities.

Two events are herein presented and their overall impact is assessed. The first workshop, organized by TUD in Darmstadt, Germany, was focused on providing a clear view of the project status to the consortium and advisory board members and receiving their professional opinion on the project activities and methodology. The second event, an ICT Security workshop was held during the NCSRD Hellenic Forum for Science, Technology and Innovation, in Athens, Greece. This event focused on presenting the methodology to a large audience of professionals and the general public.

Keywords: Workshop, Feedback, Project Impact, Dissemination, Work Package 7.

TABLE OF CONTENTS

1.1 AIMS OF THE CYBERROAD PROJECT

The CyberROAD project aims to identify current and future issues in the fight against Cyber Crime and Cyber Terrorism, in order to draw a roadmap for cyber security research. Within the two-year lifecycle of the project, a detailed snapshot of the technological, social, economic, political, and legal scenario on which Cyber Crime and Cyber Terrorism do develop will be provided. Cyber Crime and Cyber Terrorism will also be studied, in order to identify priorities and research bottlenecks.

The project relies on a large body of competences, since it has 20 partners, from 11 different countries. The consortium represents all the players and the stakeholders involved in the fight against cyber crime and cyber terrorism: law enforcement, public bodies, universities and reseach centers, as well as companies and industries. The project also relies on a high profile advisory board, made of members of worldwide relevant organizations involved in the fight against cyber crime and cyber terrorism. The wide consortium, as well as the advisory board, will ensure the involvement of all the possible stakeholders, by allowing having a clear and complete picture of the real priorities. Such a large consortium will also allow an adequate dissemination of the project results, fundamental step to foster and to promote research activity toward the directions devised during the project execution. The official project Kick-Off meeting was held in Cagliari, Italy on June 24th-25th, 2014.

1.2 PURPOSE OF THIS DOCUMENT

This document provides a comprehensive report of workshop activities conducted within the first year of the project, on par with the dissemination and exploitation strategy described within D7.1 ("Dissemination Plan and Calendar of activities").

Workshop activities are a key aspect of dissemination and exploitation efforts undertaken within CyberROAD Work Package 7. The major objective of these activities is to:

- communicate the results, progress and achievements by the project consortium,
- receive feedback by the public and the professional communities,
- utilize the feedback to improve the quality of project results,
- set up direct communication with the general public.

These activities target the following communities:

a) **the general public:** The workshops are instrumental in raising awareness on the issue of emerging Cyber Crime and Cyber Terrorism threats among the general public.

b) **the scientific community:** CyberROAD workshops enable the effective dissemination of project results to the scientific community which can also review and provide feedback.

c) **the potential stakeholders and policy makers:** including Critical Infrastructure operators, Data Protection Authorities etc. will ensure that the project's result create impact and positive influence.

1.3 STRUCTURE OF THIS DOCUMENT

This document is structured as follows:

- **Chapter 1** provides an introduction to the context of workshop activities and states the purpose of this document.
- **Chapter 2** provides a review of the workshop scope and dissemination activities.
- **Chapter 3** presents the first CyberROAD workshop in Darmstadt, Germany.
- **Chapter 4** provides a report of activities relating to the Third Hellenic Forum workshop activities.
- **Chapter 5** focuses on the results and impact of workshop activities with respect to the project.

2.1 SCOPE OF WORKSHOP ACTIVITITES

2.1.1 FIRST CYBERROAD WORKSHOP

Technische Universität Darmstadt (TUD) organized the First CyberROAD Workshop, which took place in Darmstadt, Germany from May 20th to May 21st 2015. The workshop was attended by consortium and advisory board members with a view to:

- Provide a clear view of the project's status;
- Explain the main achievements in each CyberROAD work package;
- Provide an overview of the risk assessment and research topic ranking methodology with practical examples;
- Apply and exercise the methodology;
- Receive feedback from the consortium and advisory board members;
- Inform advisory board members of the project activities in order to provide useful review.

The first CyberROAD workshop enabled the advisory board to provide in-depth review of the project activities in all Work Packages. Considering the sensitivity of information, the first workshop was restricted to advisory board members that have an official affiliation with the project.

The meeting agenda and the material provided to explain and exercise the CyberROAD methodology is appended in Chapter 6. The material provided within this deliverable has been reviewed by the Data Sensitivity Committee and is therefore considered, non-sensitive.

2.1.2 PRIVACY, SECURITY AND TRUST SESSION WITHIN THE 3RD HELLENIC FORUM

The 3rd Hellenic Forum is an annual, polythematic conference, which took place in NCSRD premises during June 29th- July 3rd, 2015, in Athens, Greece. During this event, multiple sessions and workshops took place with several talks focused on Cyber Security, Privacy and Trust. The purpose of the "Cybersecurity, Privacy and Trust" session within the Hellenic Forum was to bring CyberROAD results closer to the general public, the scientific community and Industry. The Hellenic Forum allowed the consortium to reach a wider audience with the purpose of:

- Presenting the methodology and putting it under the "scrutiny" of a large audience independent from the consortium,
- Discussing with Industry, Government and SME representatives what their specific needs and concerns in terms of Cyber Crime and Cyber Terrorism are,
- Further disseminating the CyberROAD surveys to a large audience to further increase the size of the CyberROAD knowledge base.

More than 800 registered participants attended the Hellenic Forum, with the "Cybersecurity, Privacy and Trust" session totaling more than 50 participants.

Technische Universität Darmstadt (TUD) organized a workshop and consortium meeting for the CyberROAD partners from May 20th to May 21st 2015 in Darmstadt, Germany. The agenda of the workshop included an overview of all activities in all CyberROAD Work Packages as well as a preparation for the first project rehearsal in Bruxelles on June 4th. The participants also conducted an internal training on the roadmapping methodology as well as on the methodology for the financial accounting and reporting. Also a common understading of the main project goas as well as the goals of the individual work packages should be established.

Figure 3-1 Panoramic photograph of the First CyberROAD workshop.

3.1 THE MAIN OBJECTIVES OF THE CYBERROAD PROJECT

The main objectives within WP3 of the CyberROAD project are to identify Social, Economic, Political, and Legal roots of cybercrime and to identify gaps in research topics that are important for the protection of social, economic, political, and legal rights. To accomplish this, we applied a categorization in three dimensions (socio-economic cybercrime, person-centered cybrercrime, geopolitical cybercrime) to the crimes we used as a basis for the WP5 surveys. We sketched a theoretical landscape that underpins those cybercrime enquirys and we idendified limitations of the current techniques of measuring the cots of cybercrime. Drawing on the social sciences and a range of theoretical frameworks, our study demonstrates the multi-faceted nature of cybercrime and the weaknesses of current benchmarking and standardisation approaches. Our analysis clearly shows that more work is needed to broaden a coherent conceptualisation of cyber crime to include the broad multi-faceted nature of cybercrime and from there to develop methods of data collection to benchmark and research the full dimensions of cyber crime. Our work demonstrates that there are the beginnings of a consensus on a taxonomy to describe cybercrime and gives direction as to how that taxonomy may develop.

Figure 3-2 Start of the exercise session of the First CyberROAD Workshop.

Within WP4, we focused on the technological aspects of cybercrime. Our work is centered on Hardware, Software and Trends we used to idendify upcoming high level scenarios. Those are currently: Smart cities, Internet of Things/Everything - Quantified self, Mobile Biometry, Unmanned systems, Smart transportation, Location based services, Social Networks, Bring your own device, Virtualization, Cloud Computing, Auto Tagging and Smart energy grids. Based on those scenarios, we are now identifying the assets in those scenarios that need to be protected as well as the risks and attacks on those assets. We will also evaluate the current technologies and efforts to protect those assets.

Within WP5, we completed a survey of 192 participants focusing on the effects of person-centered cybercrime on participants aged between 18 and 35. Our results show that while the fear of cybercrime is high, the effects felt are minimal. This raises the question whether the particular focus on apsects of cybercrime is driven by an IT industry imperative rather then by the lived experience of people. Stakeholder needs and interests need more investigation. Drawing on the social sciences and a range of theoretical frameworks, our study demonstrates the multi-faceted nature of cybercrime and the weaknesses of current benchmarking and standardisation approaches. Our analysis clearly shows that more work is needed to broaden a coherent conceptualisation of cyber crime to include the broad multi-faceted nature of cybercrime and from there to develop methods of data collection to benchmark and research the full dimensions of cyber crime Our work demonstrates that there are the beginnings of a consensus on a taxonomy to describe cybercrime.

3.2 *ROADMAPPING METHODOLOGY & EXAMPLES*

During the meeting the roadmapping methodology was presented, discussed and later on some examples were developed. The roadmapping methodology is based on a scenario building and gap analysis process, which can be seen in the following figure from the workshop (Figure 3-3).

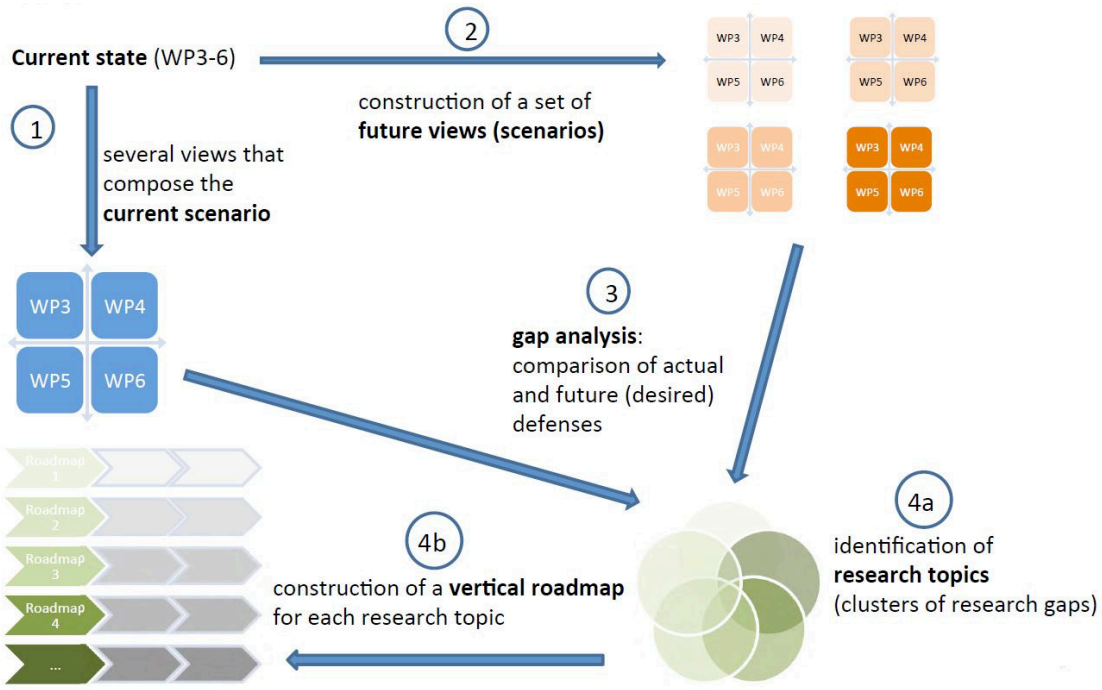


Figure 3-3 Scenario Building in CyberROAD.

In a first step several views for current scenarios have to be composed, which means, that scenario templates have to be filled with a description of the scenario, possible threats and a list of desired defenses. Besides this also key driving factors that are expected to influence the development of future scenarios may be included. Based on this also a list of future views (future scenarios) have to be constructed. During the workshop three possible future views were sketched (Private Transportation Systems, Social Networks and Cloud Services). In the following figure (Figure 3-4) the view for Private Transportation is shown:

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 store daily movements (presence and destination).
- Latest news and other 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.
- Such an infrastructure is also open to **private advertisements**, to amortize the costs.
- Monthly transport is calculated by an **app on the user's mobile phone**, which automatically connects to the car, enables the user to use it and exchanges data about journey duration. Only the mileage is recorded; 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 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

Figure 3-4 View example in CyberROAD.

After this the gap analysis (3) process is performed, which means that the threats and defenses of the current and future views are compared and research gaps are identified. During this process threats may increase, decrease, disappear or even new threats may come into our scope (see Figure 3-5).

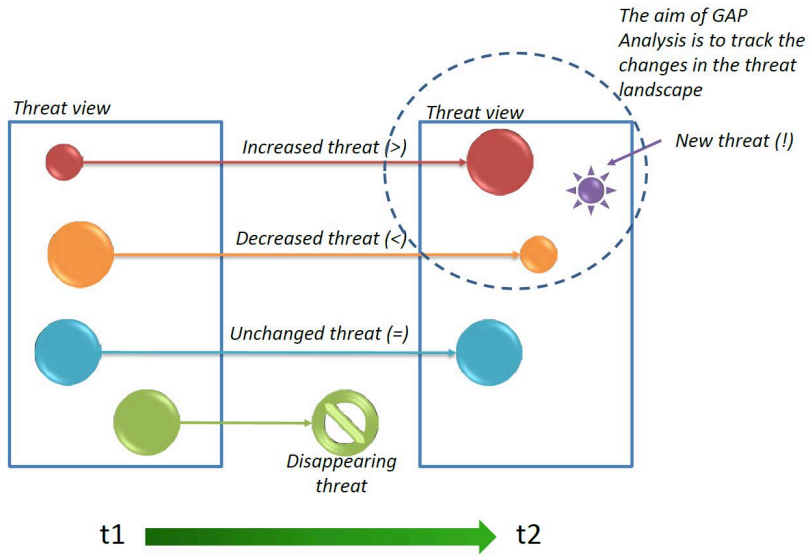


Figure 3-5 Current and Future Views example shown explained in the CyberROAD exercise session.

For instance the gap analysis for our transportation scenario could look as follows:

GAP #	Views	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
1	Transportation Systems	Malware coming from the mobile device connected to the car infotaiment 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.	- Mobile anti-malware software - Network based Intrusion Detection Systems	Intrusion detection systems able to identify anomalous traffic flowing through the CAN Bus.	**Malware detection in unconventional environments**

Figure 3-6 Example of CyberROAD gap analysis.

From the list of identified gaps coherent clusters of related research gaps can be built and by doing so a set of research topics can be identified (4a). These topics then are priorized and afterwards lead to the final CyberROAD roadmap (4b). The resulting roadmap consists of a vertical roadmap for each of the mentioned research topics.

3.3 *ROADMAPPING METHODOLOGY TRAINING*

During the roadmapping methodology training session, CyberROAD partners were subdivided into three different working groups, each one including representatives from WP3, WP4, WP5, and WP6; Each group practiced with the roadmapping methodology, building the current state, developing future scenarios and views and identifying possible research gaps.

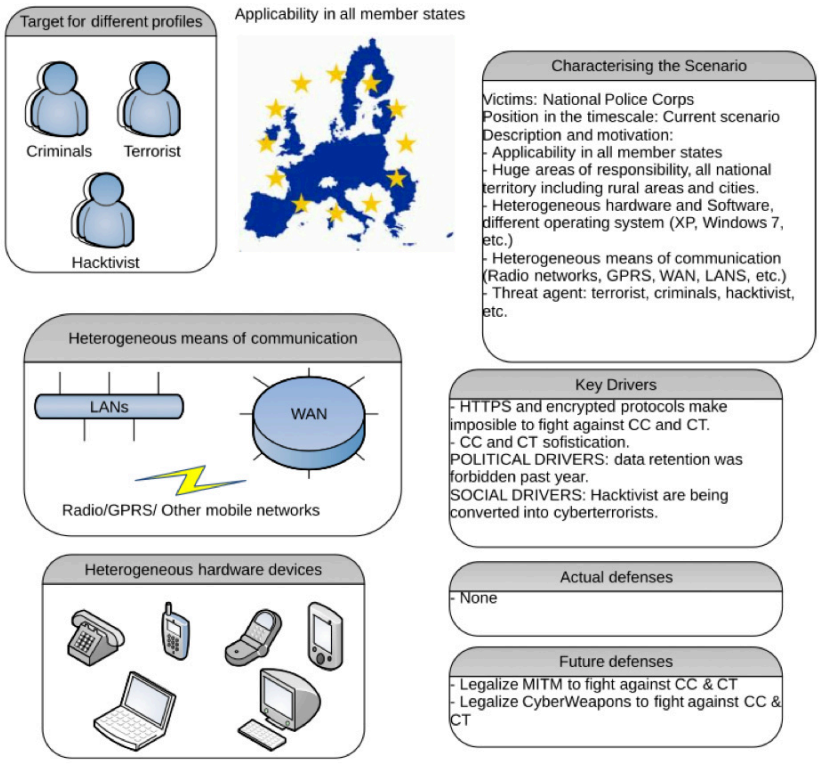


Figure 3-7 Example scenario developed during the First CyberROAD Workshop.

The above figure shows a National Police Corps scenario, which has been proposed by INDRA. The scenario illustrates the current National Police Corps, which are responsible for huge areas in each country, including rural areas. The used hardware is very heterogeneous because a wide variety of hardware and software is used. This also applies to the communication media, which can range from mobile networks to LANs and WANs. The scenario and the threat agents may be applicable to all member states.

Key drivers for this scenario are the emerging technological capabilities of the threat agents. For instance fighting cyber crime becomes more and more difficult due to encrypted communication protocols. From this on the current and future defenses are illustrated.

The Integrated Systems Laboratory (Institute of Informatics and Telecommunications, National Centre for Scientific Research Demokritos - NCSRD) organized a 3-day ICT workshop during the 3rd Hellenic Forum, spanning a variety of thematic areas. NCSRD, as a CyberROAD partner, selected "Cyber Security, Privacy and Trust" as a key thematic area, to be discussed during the first day of the ICT workshop (June 29th, 2015). The Cyber Security, Privacy and Trust session featured talks[1] on:

- Social Media Intelligence in practice: The NEREUS experimental platform - Prof. Dimitris Gritzalis
- Cyber Defence from the NATO Allied Command Operations Perspective - Commander Georgios Chatzichristos
- Cyber Defence Exercises: Lessons Learned? - Mr. Konstantinos Zografos
- Preparing a research roadmap for Cyber Security, Privacy and Trust - Dr. Olga Segou

Figure 4-1 Third Hellenic Forum session on ICT & Security.

The project website and social networking accounts were utilized to disseminate information on the First CyberROAD Workshop as well as the 3rd Hellenic Forum. External communication channels were also utilized. In the case for the Hellenic Forum, personalized invitations were also sent.

[1] Presentations available at: http://events.demokritos.gr (Accessed September 2015).

Figure 4-2 The Hellenic Forum page in the European Commision portal.

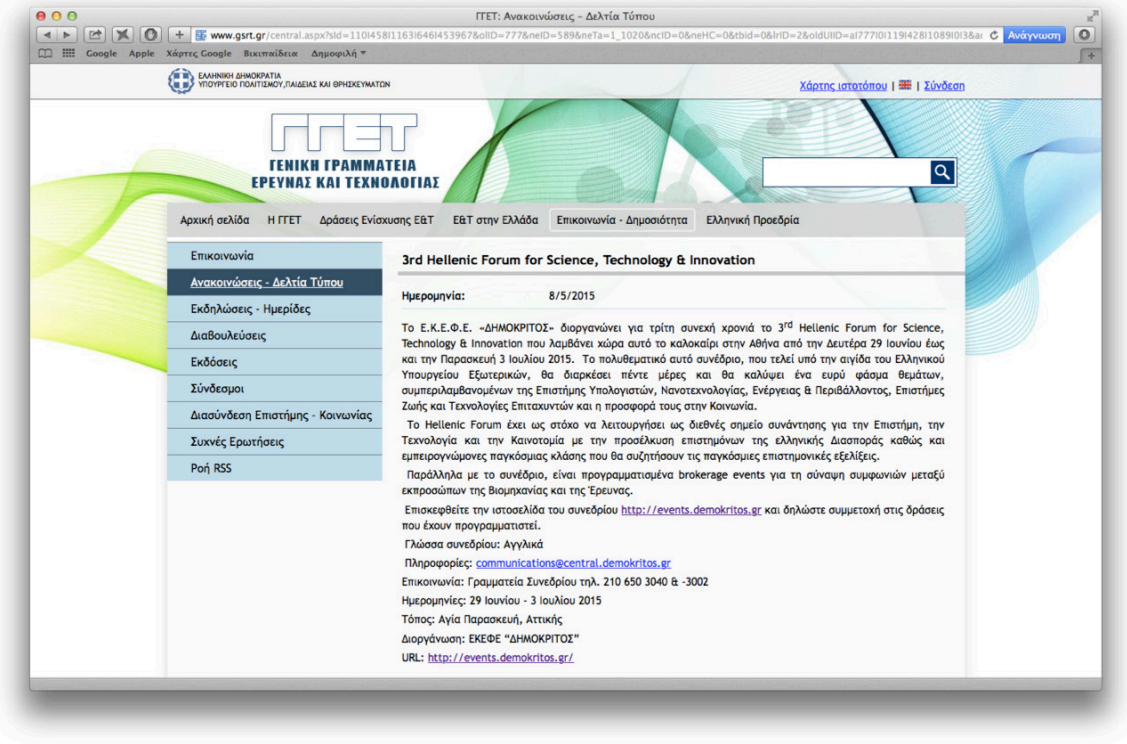
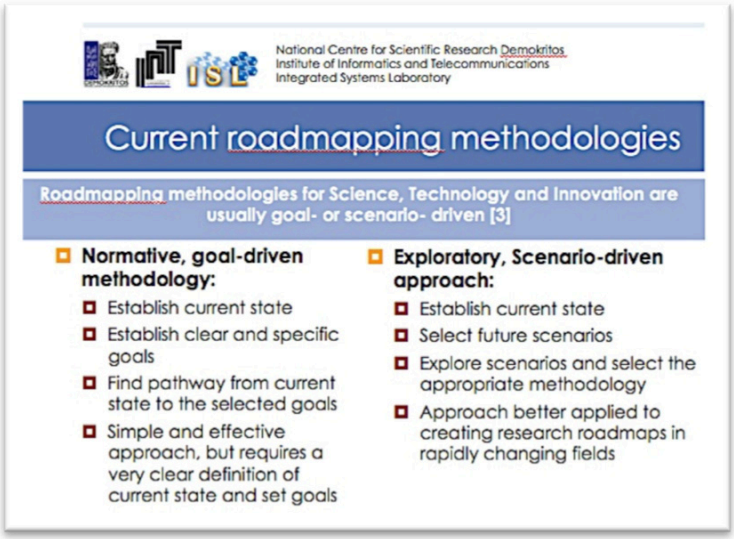


Figure 4-3 The Hellenic Forum page in the website of the Hellenic General Secretariat for Research and Technology (with the support of the Hellenic Ministry of Education).

4.1 CyberROAD PROJECT SESSION AND DISCUSSION

In the massive and ever-changing field of Cyber Security, prioritizing among research topics remains a challenging task. Within the Hellenic Forum, NCSRD gave an overview of the CyberROAD project approach which takes into account:

- Cyber crime and cyber terrorism, (targeting organizations, the public or critical infrastructures)
- Emerging, cutting-edge technologies and commercial trends
- Ethical and Legal implications and gaps in current regulations
- Currently set EU policies on the development of Transport, Security etc.



NCSRD presented the project activities especially in terms of the roadmapping methodology. The importance of cyber crime research was highlighted as the economic impact of worldwide cyber crime was brought into the discussion with the audience.

According to recent reports[2],[3], the annual cost stemming from cybercrime activities reaches 400 Billion Euro, which reaches considerable amounts of EU or individual countries' GDP. There is, however, a profound lack of research funding for cyber security solutions. CyberROAD roadmapping aims to help prioritise among research topics and thus help optimize the financial investment to research.

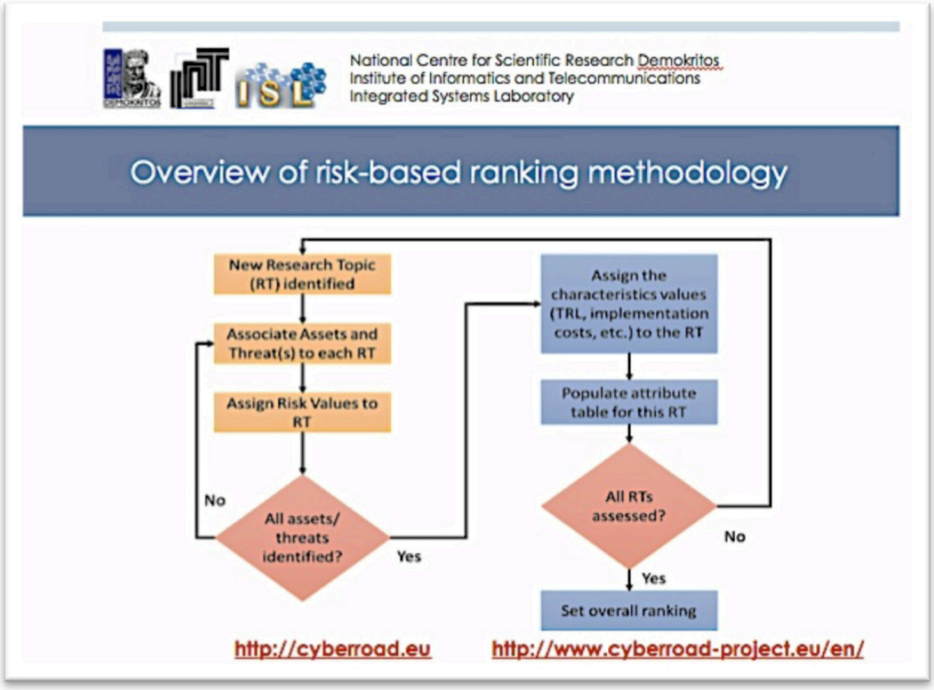
The most relevant roadmapping methodologies[4] were introduced to provide the basis and the needed context for the discussion. Goal-driven methodologies are usually simple and effective but require a good

[2] Raj Samani, "4 Hidden Economic Costs of Cybercrime", Intel Security, http://www.securingtomorrow.com/blog/knowledge/4-hidden-economic-costs-cybercrime/

[3] Inter Security and McAffee Report, "Net Losses: Estimating the global cost of cybercrime", Center for Strategic & International Studies, June 2014.

[4] Martin Moehrle, Ralf Isenmann, Robert Phaal, "Technology Roadmapping for Strategy and Innovation: Charting the Route to Success", Springer Science & Business Media.

understanding of the final goals and the current state. Therefore, goal-driven roadmapping would not be sufficiently accurate in an ever-changing field of cyber security, as cyber crime keeps evolving and new threats are revealed. In contrast, a scenario-driven approach allows the exploration of multiple scenarios. CyberROAD's scenario-driven approach based on current day cyber crime and on future predicted trends was presented and discussed.



This approach is complemented with a risk assessment methodology, which associates each scenario and each research topic to the risks it addressed and its possible impacts (e.g. financial risk, health and safety etc).

Examples were discussed based on a Transport scenario with two suggested research topics. The first research topic was focused on Intrusions to Command and Control systems of a railway operator, while the second was the creation of panic through social media misinformation. The attendees were asked to provide examples of threats they face currently or threats they expect to be facing in the future.

The attendees were invited to participate to the CyberROAD surveys and to have a discussion on what challenges they face with respect to Cyber Crime and Cyber Terrorism.

4.2 TOPICS DISCUSSED

Participants representing SMEs and Industry were particularly concerned on **Cyber Readiness and Awareness Training**. There was an expressed need to **assess the overall vulnerability** of an organization in a technical level and in the level of human resources. SMEs expressed needs to have appropriate tools to assess their overall vulnerability to cyber crime and to be able to **quantify or assess the economic impact, impact to reputation** etc., including means to **optimize their security investments**, given limited funds.

Invited speakers from the Hellenic Ministry of Defense (CyberROAD partner) and NATO SHAPE, delivered presentations on the importance of training and the need for large-scale cyber security exercises. Lessons learnt from results of the exercises were discussed and the need to develop national cyber security agendas, including **raising awareness** of the proper way to report cyber crime and cyber terrorism occurences to national authorities. Participants discussed their respective organizations' needs on a cyber crime and cyber terrorism strategy based on lessons learned from large-scale cyber security exercises. The identified topics included:

- **Security and safety of autonomous systems** such as Unmanned Aerial or Ground Vehicles (UAVs/UGVs);
- Improving the **resilience of telecommunications** components from Physical Layer attacks (Intentional Electromagnetic Interference, Signal jamming/spoofing, etc) with focus on Software Defined Radio (SDR) systems that rely on spectrum sensing.
- Combating **ransomware attacks**, where a user's files are maliciously encrypted and the users are prompted to pay a fee to a cyber criminal in order to release the files.
- Raising awareness on the proper channels to report cyber crime and cyber terrorism incidents and cyber security failures, as well as the need for **improved Security Information and Event Management** (SIEM) systems.

Furthermore, all participants expressed concern over the rise of violent radicalization. Most participants considered the **Internet as a facilitator and "catalyst" for radicalization**. Massive data mining on social media accounts from Law Enforcement agencies was considered as a solution, although it was not particularly welcome due to the privacy and human rights implications.

After the first CyberROAD workshop in Darmstadt, the audience (comprising consortium members and external invited advisors) had a general overview of the project activities as well as the status and key accomplishments and achievements of the project. The first workshop recapitulated the roadmapping methologies that are used in the CyberROAD project. Practical examples were presented and discussed. This activity was especially significant, since roadmapping is a very broad topic without many fixed rules. The practical exercise was considered a very positive effort and an important part of the workshop, allowing the harmonization of the project activites and allowing the external participants to fully understand and review the scope of the CyberROAD methodology. Furthermore, during the first workshop the participants provided feedback and a detailed review of project activities across all Work Packages, which also includes the overall status of the project.

During the Hellenic Forum workshop, consortium members were able to discuss the methodology and the project's key results with representatives from Research/Academia, Industry, Government and SMEs. The audience provided input on what their specific needs and concerns in terms of Cyber Crime and Cyber Terrorism are, and offered examples of future scenarios to be considered. Furthermore, the CyberROAD surveys were disseminated to a larger audience, further increasing the participation and improving availability of survey data.

The following table consolidates the results and the feedback collected within these activities. To summarise, there was an identified need to harmonise the suggested taxonomies and show how Social, Ethical, Political, Legal analysis fits within the CyberROAD methodology in a more formalized way. Table I also collects the variety of future scenarios that were proposed for research in the two events. According to the input we collected, the proliferation of sensor networks has created the need to safeguard privacy and secure Critical infrastructures against Cyber Crime and Cyber Terrorism. The security of Autonomous Systems against cyber attacks was also considered as a major theme to explore. The use of the Internet and for the purpose of Cyber Terrorism and as a catalyst for radicalization and the creation of Insider Threats was mentioned as an important scenario for future research.

Table I: Results & Impact of Workshop activities per WP		
WP2	Scientific Coordination	The project roadmapping methodology was presented in both events. During the first event in Darmstadt (see Chapter 3): • SUPSI provided an overview and a "training programme" with activities designed to ensure the full alignment of the consortium with respect to the roadmapping methodology. • Consortium members and external advisors discussed given examples and asked to exercise the methodology. A scenario on Lawful Interception was designed as an exercise and additional scenario where discussed. During the second event in Athens (see Chapter 4): • An overview of the risk assessment methodology was presented to a larger audience comprising of representatives from academia, government, stakeholder organisations and the commercial world. • CyberROAD created the chance to discuss their individual needs and concerns regarding cyber crime, cyber terrorism and cyber security in general. • Future scenarios were discussed with the audience after the end of the workshop.
WP3	Social, Economical, Political and Legal Scenario	• CyberROAD needs to clarify how the Societal/Legal/Ethical/Economical/Political landscape fits into the roadmapping methodology. • During the Darmstadt meeting explicit references were made on Cyberterrorism, as a category of Geopolitical cybercrime and additional focus was required on Cyber Terrorism and online radicalization. • During the Athens workshop, the assessment of privacy and trust implications were discussed and specifically how the perception of privacy and trust can affect a security technology's adoption. • An issue to consider is also the difference in public perception and expert opinion in terms of privacy and data protection issues.
WP4	Technological Scenario	• In terms of Critical Infrastructure protection, it was discussed that the project should be broadened in scope. • Focus on Industrial Control Systems is adequate.
WP5	Cyber Crime	• The presented taxonomies for Cyber Crime and Cyber Terrorism should be better aligned with each other. • CyberROAD should clarify what differentiates the project taxonomy from the others publicly available and how/why the proposed taxonomy could be accepted.
WP6	Cyber Terrorism	

Table I: Results & Impact of Workshop activities per WP	
Across all WPs	Possible themes were suggested for CyberROAD scenarios in both events: • Lawful Interception Systems Use & Misuse, • Obsolescence of the Utility Network, • Security & Privacy issues in the Internet of Things, with a particular focus on Smart Cities, • Security of Autonomous Systems, • Security of "Everything as a Service", • Spoofing and manipulating data in sensor networks and Internet of Things, • Security of Software Defined Radio (SDR) Systems, • Privacy and Trust in the digital age, with respect to massive data mining by law enforcement, • The Internet as a "catalyst" for radicalization, • Cyber Security awareness training tools for SMEs. • Security and Privacy frameworks for dual-use technologies. • Combating ransomware attacks

The social impact of the project increased tangibly as participants in the workshop activities discussed the project activities via social media. As described in D7.1, a Klout account has been set up to monitor the impact of the project's social media accounts. The following figure (Fig 5-1) illustrates a 90-day Klout score history. A slight increase is observed during the Darmstadt workshop, while a significant increase was measured during the Hellenic Forum activities. This increase was expected, as the Hellenic Forum was a public event that gathered a large audience. The amount of mentions and posts regarding the project during the days of the Hellenic Forum has effectively contributed towards the dissemination of the project goals and key results and also created a surge of visitors to the CyberRoad Website.

Taking into account the results and the feedback gathered, we surmise that CyberROAD workshop activities managed to accomplish the intended goals (described in section 2) and particularly succeeded in:

- Explaining the main achievements of the project to a variety of stakeholders and the public;
- Providing an overview of the risk assessment and research topic ranking methodology with practical examples and receiving feedback on the overall methodology;
- Harmonising all CyberROAD activities with the proposed methodology and with stakeholder needs;
- Allowing participants to apply and exercise the methodology and provide their own examples of future scenarios;
- Presenting the methodology and putting it under the "scrutiny" of a large audience independent from the consortium.

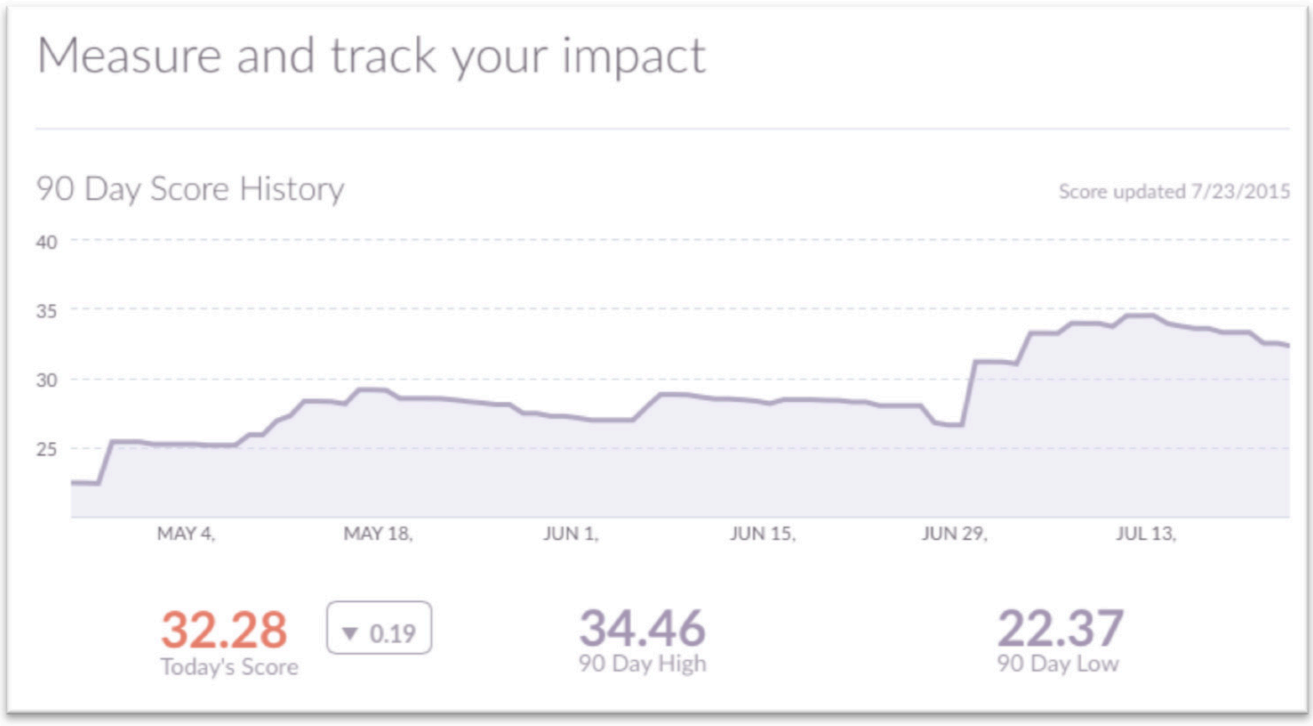


Figure 5-1 Klout score variations for May-July 2015, showing a significant increase in social impact, particularly after the public ICT workshop within the Hellenic Forum.

Figure Reference

Attached Documents

- Darmstadt Meeting: Agenda
- Darmstadt Meeting: Slides on Methodology
- Darmstadt Meeting: Slides on Methodology examples

Darmstadt, Germany

May 20-21, 2015

Place

TU Darmstadt | 3th floor

Mornewegstrasse 30

64293 Darmstadt

Meeting called by Fabio Roli – Project Coordinator

Attendees

- CEFRIEL
  - Enrico Frumento, Federica Freschi
- CYBERDEFCON
  - Jart Armin, Bryn Thompson
- FORTH
  - Elias Athanasopoulos
- GOVERNO DE PORTUGAL - Polícia Judiciária
  - Cristina Farinha
- HELLENIC REPUBLIC - Ministry of National Defence
  - Colonel George Beldecos (1st day), Major Isidoros Monogioudis
- INDRA
  - Javier Martínez Torres
- INOV
  - John Rodrigues
- McAFEE
  - Igor Muttik
- MELANI
  - Clement Guitton
- NASK
  - Piotr Kijewski
- NCSRD
  - Olga Segou, Stelios Thomopoulos
- POSTE ITALIANE
  - Massimiliano Aschi
- UNICA
  - Davide Ariu, Giorgio Giacinto, Fabio Roli
- PROPRS
  - Carlo Dambra
- ROYAL HOLLOWAY – University of London
  - Anja P. Jakobi
- SBA RESEARCH
  - Peter Kieseberg
- SECURITY MATTERS
  - Massimo Guadagnoli
- SUPSI
  - Angelo Consoli
- TECHNISCHE UNIVERSITAET DARMSTADT
  - Erik Tews, Stefan Katzenbeisser, Christian Schlehuber
- VITROCISET
  - Francesco Carpine, Giovanni Guardi

DAY 1	Wednesday May 20th, 2015 **Preparation of the review meeting**

Session 1

9.00 A.M. – 9.20 A.M.
UNICA
	• Overall project update
	• Presentation of the review meeting in Brussels
	  ○ Reviewers
	  ○ Agenda
	  ○ Duties
	• Update on the WP1 Activities

9.20 A.M. – 10.00 A.M.
SUPSI
	• **Update on the WP2 Activities**
	  ○ Report on the 1st year activities (**20 minutes**)
	  ▪ Tasks and deliverables: status, issues, and deviations from the DoW
	  ○ Toward the 2nd year (**10 minutes**)
	  ▪ Update on the deliverables due in the second year: current status
	  ▪ Plans for the finalisation of deliverables due in the 2nd year:
	  - Actions & deadlines (WP leaders are requested to obtain them from the task leaders)
	  ○ Questions and comments (**All**) (**10 minutes**)

10.00 A.M. – 10.40 A.M. **RHUL**	• **Update on the WP3 Activities** (as for WP2)
10.40 A.M. – 11.00 A.M.	**Coffee break**

Session 2

11.00 A.M. – 11.40 A.M. **INDRA**	• **Update on the WP4 Activities** (as for WP2)
11.40 A.M. - 12.20 P.M. **CYBERDEFCON**	• **Update on the WP5 Activities** (as for WP2)

12.20 P.M. - 1.00 P.M. **PJ**	• Update on the WP6 Activities (as for WP2)
1.00 P.M. – 2.30 P.M.	**Lunch break**

Session 3

2.30 P.M. – 3.10 P.M. **NCSRD**	• Update on the WP7 Activities (as for WP2)
3.10 P.M. – 3.30 P.M. **UNICA**	• Mid-term financial reporting
3.30 P.M. – 4.15 P.M. **UNICA**	• CyberROAD roadmapping methodology o 3.30 – 4.15 Presentation of the methodology
4.15 P.M. – 4.35 P.M.	**Coffee break**

Session 4

4.35 P.M. – 5.05 P.M. **CEFRIEL**	• **CyberROAD roadmapping methodology** o Using the methodology to identify research gaps: an example
5.05 P.M. – 5.30 P.M. **UNICA, ALL**	• **CyberROAD roadmapping methodology** o Discussion and introduction to the training session

DAY 2	Thursday May 21th, 2015 **Toward the CyberROAD roadmap**

Session 1

9.00 A.M. – 9.15 A.M. **UNICA**	• Introducing the CyberROAD advisors
9.15 A.M. – 10.45 A.M. **UNICA, WP LEADERS**	• Simulation of the review meeting in Bruxelles
10.45 A.M. – 11.15 A.M.	**Coffee break**

Session 2

11.15 A.M. – 1.00 P.M. **ALL PARTNERS**	• **Roadmapping methodology: training session.** o CyberROAD partners will be subdivided into three different working groups, each one including representatives from WP3, WP4, WP5, and WP6. o Each group should practice with the roadmapping methodology, building the current state, developing future scenarios and views and identifying possible research gaps.
1.00 P.M. – 2.30. P.M.	**Lunch break**

Session 3

2.30 P.M. – 4.00 P.M. **ALL PARTNERS**	• **Results of the training session and discussion** o Presentation of the training session outputs o Discussion
4.00 P.M. – 4.15 P.M.	• AOB • Final remarks

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

The roadmapping methodology: creation of roadmaps based on scenario analysis

Darmstadt, May 20th, 2015

Why roadmapping?

- The project call: Topic SEC-2013.2.5-1 Developing a Cyber crime and cyber terrorism **research agenda**
  - .....
  - What are the major research gaps?
  - What are the challenges that must be addressed?
  - ……

- **Research agenda**: we are committed to do a **roadmap** (DoW B1.1.3 – Objectives)
- The DoW committs us to develop a **roadmapping methodology** (WP2)

How to do the roadmap?

SEPL & TECHNOLOGY CURRENT STATE

- **T3.1** SOCIAL, ECONOMIC, POLITICAL, LEGAL LANDSCAPE
- **T3.2** STAKEHOLDER NEEDS
- **T4.1** TECHNOLOGY LANDSCAPE
- **T4.3** SECURITY ANALYSIS OF CRITICAL INFRASTRACTURES

SEPL & TECHNOLOGY FUTURE STATE

- **T3.3** SEPL research topics
- **T4.2** New and emerging technologies

CC&CT CURRENT STATE

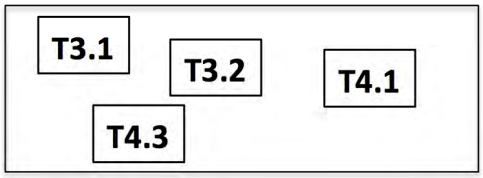
- **T5.1**
- **T5.2**
- **T6.1**
- **T5.3**
- **T6.3**

CC&CT FUTURE STATE

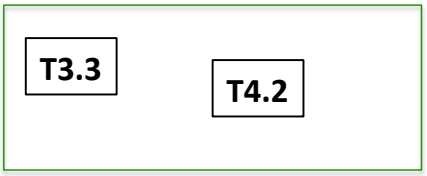
- **T5.4**
- **T6.6**
- **T6.5**

How to do the roadmap?

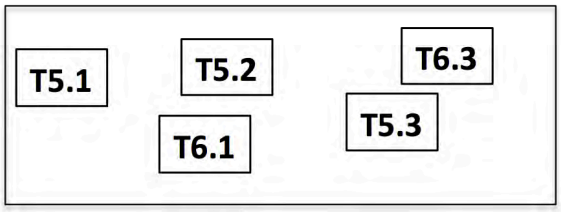
SEPL & TECHNOLOGY CURRENT STATE



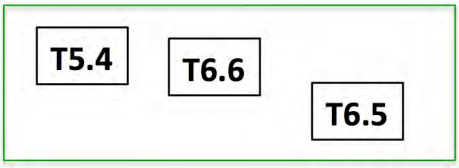
SEPL & TECHNOLOGY FUTURE STATE



CC&CT CURRENT STATE



CC&CT FUTURE STATE



- We already have the basic ingredients to create **exploratory roadmaps** based on **scenario building** and **gap analysis**

About this presentation

Based on the documents:

- "*Tutorial on Scenario Analysis & Roadmapping*", April 23rd, 2015
- The companion slides "*Creation of roadmaps based on scenario analysis*", confidential internal document, version 1.0, March 13, 2015

Sequel of the previous documents on the roadmapping methodology:

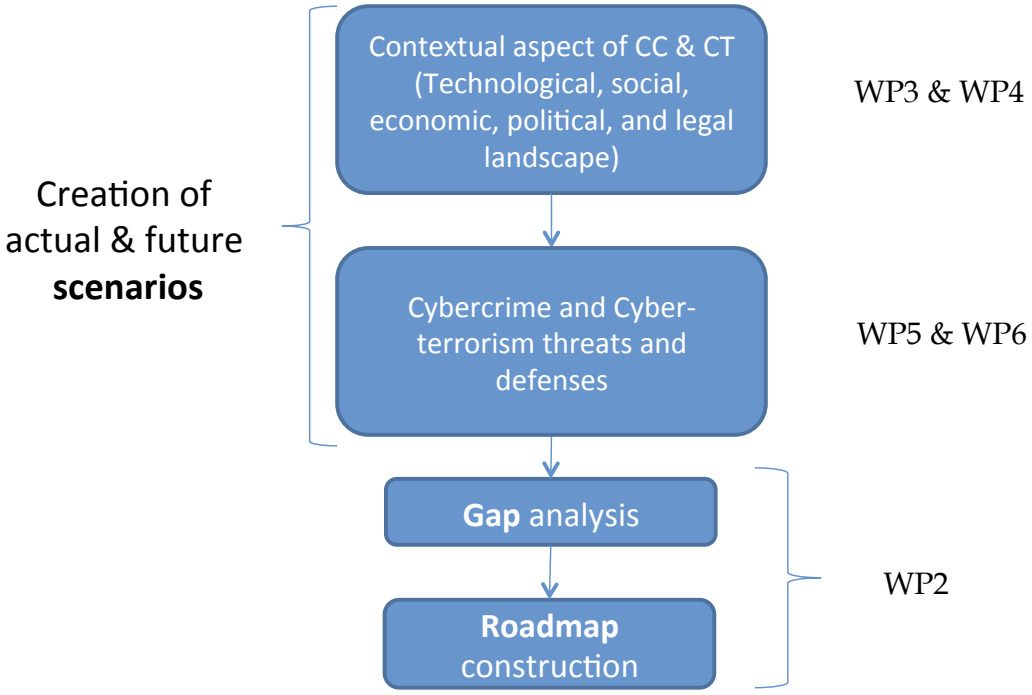
- D2.1: *Roadmapping Methodology and Guidelines for Information Collection and Assessment*
- *Toward the CyberROAD roadmap,* confidential internal document (slides, October 2014)

Aim of this presentation

- We describe a complete methodology to develop *vertical*, exploratory roadmaps, based on **scenario building** and **gap analysis**
  - the methodology revises state-of-art techniques that have been applied to other domains, see references

- We give simple examples of its application
  - PROPRS (Carlo Dambra) will give more details on the "ranking" methodology and CEFRIEL (Enrico Frumento) will describe an example of application

Main steps of CyberROAD roadmapping



Scenario building (1/3)

A widely used approach in exploratory roadmapping (see Refs.)

In the Cyber ROAD context:

- **SCENARIO**
  a concise and schematic representation of the actual or of a future **state**, aimed at identifying **threats** and **defenses**

- **STATE**
  - the whole set of technological, social, economic and political conditions that define the *context* of CC and CT
  - the corresponding specific threats and defenses

- **THREATH**
  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, etc.), with the potential to either stop or mitigate a threat, or to make its legal prosecution easier

Scenario building (2/3)

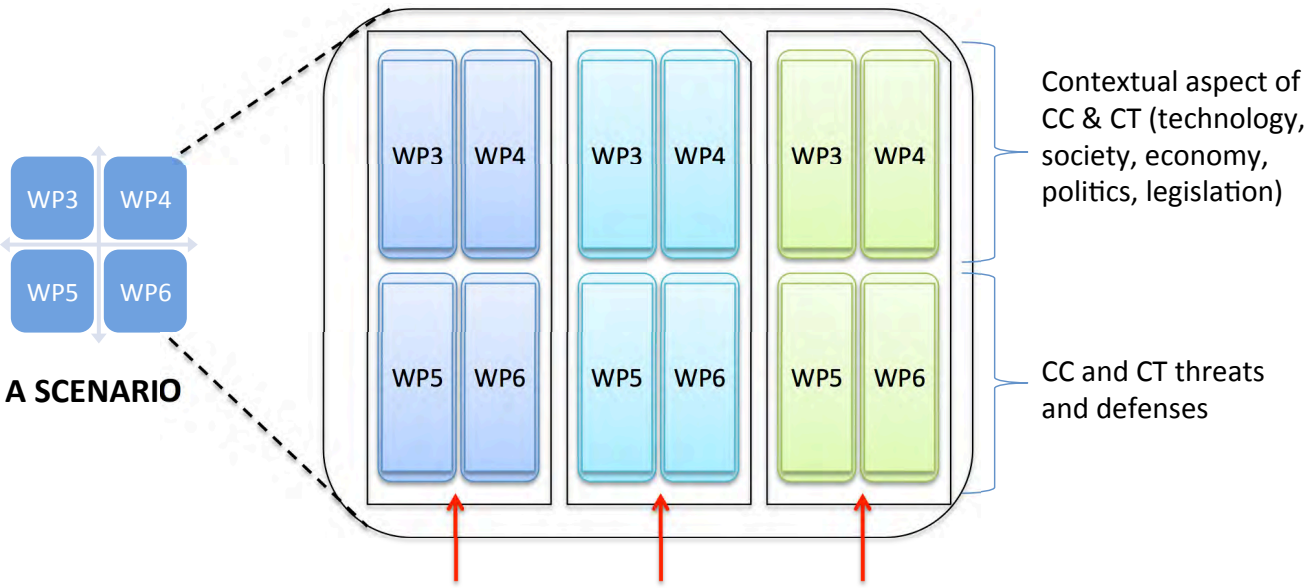
A scenario can be made up of several ***vertical*** **sub-scenarios**, or **views**.

Each view focuses on a specific aspect of the current/future state, e.g.:

- Workforces
- Social Networks
- Cloud Services
- Private Transportation Systems
- Payment Systems
- Driverless Vehicles
- Mobile Devices and Services

Scenario building (3/3)

An example:



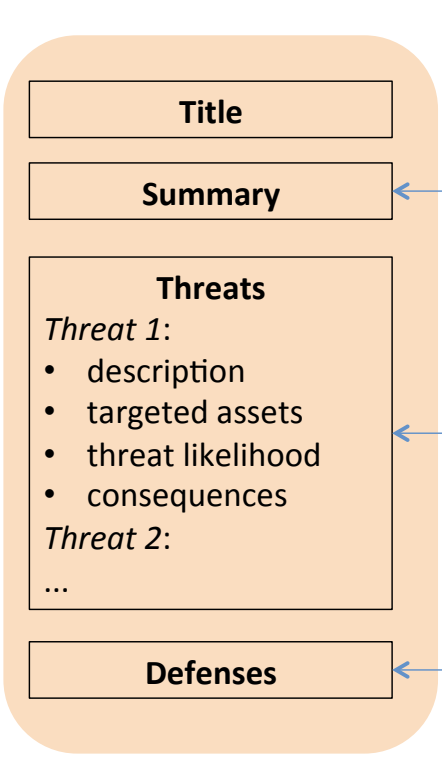
Views are defined by WP3-WP6, under the coordination of WP2

VIEW: **Social Networks**

VIEW: **Cloud Services**

VIEW: **Private Transportation Systems**

Scenario template (1/4)



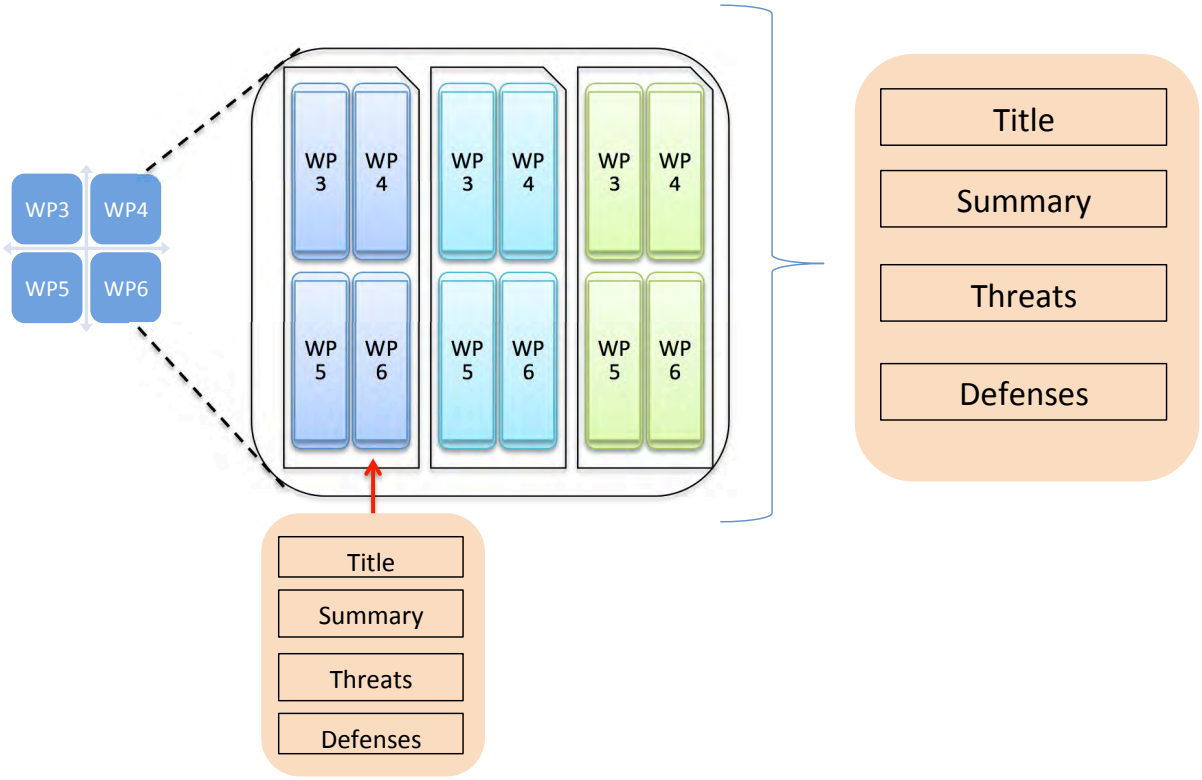
a **one-page** narrative description

a list of the threats which emerge from the scenario, including attributes required by PROPRS' Risk Assessment Ranking Methodology (Task 2.2)

a list of the desired defenses

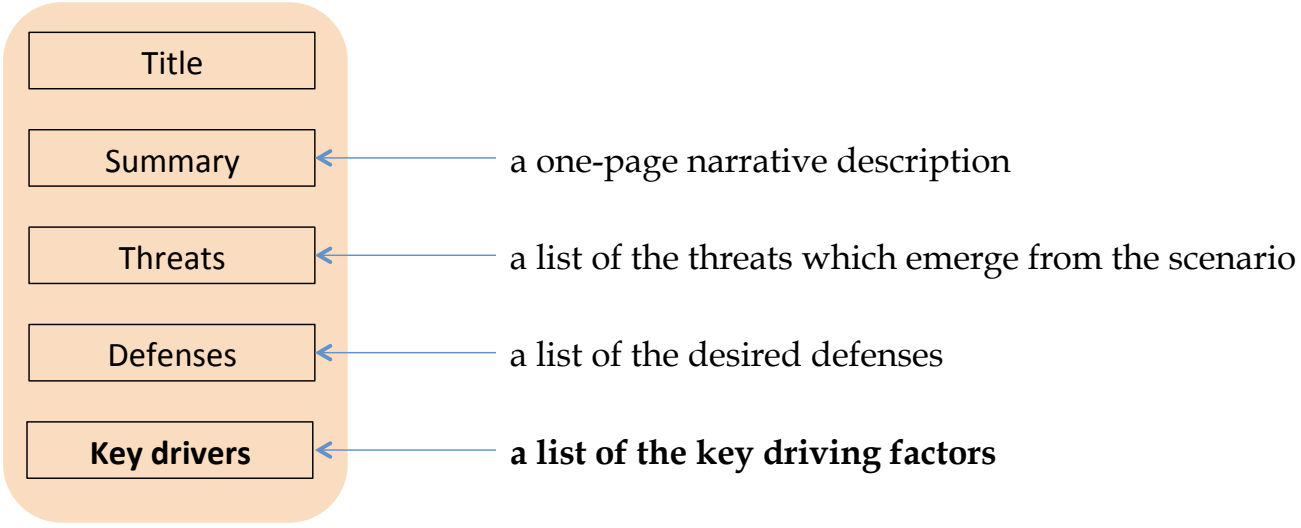
Scenario template (2/4)

Both a **whole scenario** and a **single view** can be described using the same template.



Scenario template (3/4)

The template of the **current** scenario may be enriched with a slot containing the **key driving factors** (**drivers**) that are expected to influence the development of future scenarios.



Scenario template (4/4)

Scenario / View

Summary (one page): ... ***possible elements to be addressed:***

Contextual environment (WP3)

- Society (e.g. how the society look like, role of individuals and communities, internet governance, identity management, etc.)
- Political system and climate (e.g. societal and democratic values, governance value, transparency, security, etc.)
- Economic climate (e.g. employment, age composition of labour force, ubiquitous workforces, personal data selling business models, etc.)
- Legal and Law enforcement issues (skills of the law enforcement, jurisdiction, (personal) data protection and liability, IP, etc.)

Technology & (technology enabled) services (WP4)

- ICT available: which kind of technology will we be using in 2020? (Payment systems, Mobile devices, IoT, Sensors & wearables, etc.)
- Services: which kind of services will we be using in 2020? How the current services will evolve in the next 5 years? (Communication service providers, Content service providers, Cloud service providers, Reputation and cyber risk management/insurances, etc.)

Cybercrime & Cyberterrorism specific issues (WP5 and WP6)

- Offensive technologies (malware evolution, spam generation, social engineering, etc.)
- Defensive technologies (intrusion & malware detection, spam filteringetc.)
- Programming techniques & ARM coding
- Business models, Marketplace blackmarkets, Targets

Possible key driving factors (only for the **current** scenario): ...

Threats		**Desirable countermeasures**
Threat 1	Threat description	Desirable countermeasures for threat 1
	Assets targeted by the threat	
	Threat likelihood	
	Consequences of the threat	
...	...	...

Example of Actual State (1/2)

Summary (one page)

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. ...

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. ...

Cloud and social platform are accessed also through a number of **wearable devices** (e.g. watches). The availability of cheap, powerful hardware (CPUs, sensors, transmitters) is enabling a number of different **applications**: Home Automation, e-Health, Transportation systems, UAV; research on self-driving cars is still ongoing. ...

Example of Actual State (2/2)

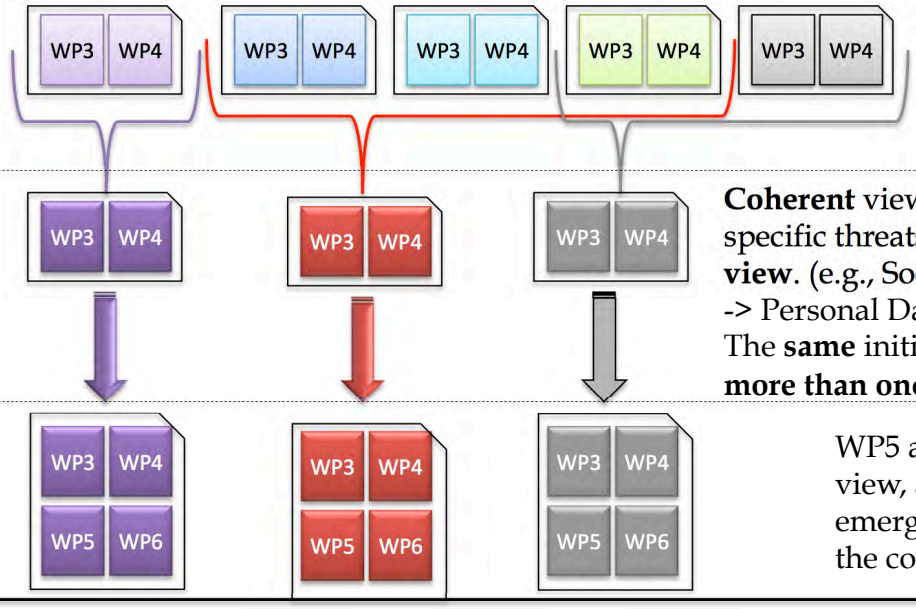
Threats:

- 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 LEA to get access to the users' data stored in the cloud, and 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)
- Crypthography used to encrypt data stored in the cloud
- Anti-malware solutions for both desktop and mobile platforms

How to build views



Views (i.e., partial scenarios) focused on specific **contextual aspects** (Sources: WP3 and WP4 + ARES Workshop)

Coherent views that can interact resulting in specific threats, are combined into a **single view**. (e.g., Social Networks, Cloud Services -> Personal Data Management.
The **same** initial view can be included into **more than one** final view.

WP5 and WP6 complete each view, adding **threats** that can emerge from the context, and the corresponding **defenses**

GOALS

Title
Summary
Threats
Defenses

Title
Summary
Threats
Defenses

Title
Summary
Threats
Defenses

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

Examples of Future Views (1/4)

Three possible future views are sketched:

- Private Transportation Systems
- Social Networks
- Cloud Services

Examples of Future Views (2/4)

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 store daily movements (presence and destination).
- Latest news and other 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.
- Such an infrastructure is also open to **private advertisements**, to amortize the costs.
- Monthly transport is calculated by an **app on the user's mobile phone**, which automatically connects to the car, enables the user to use it and exchanges data about journey duration. Only the mileage is recorded; 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 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

Examples of Future Views (4/4)

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)
- Absence of supranational regulations: it is hard for LEA to access the users' data stored in the cloud in case of crime, severely limiting their capability to prosecute certain categories of crime

Desired countermeasures:

- Situational security authentication (based on human and machine behaviour)

Examples of Future Views (4/4)

View Title: Cloud Services

Summary:

User wants to **complete a task in any possible place** and **over any possible device**. The availability of large and long bandwidth makes such services available to more than 90% of the EU citizens.

The EU is now moving toward a complete **dematerialization of the personal dataspace** on cloud services, 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:

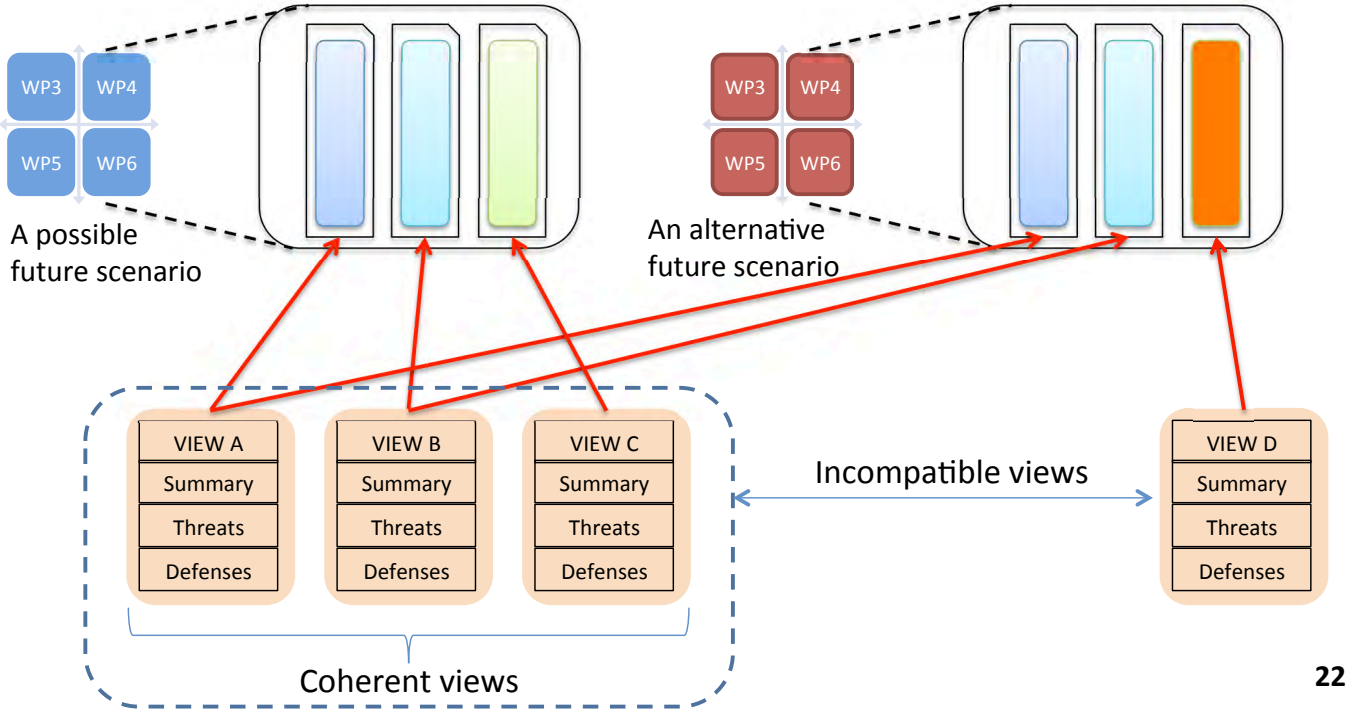
- Behaviour theft (like nowadays the identity theft)
- Cross-border legal problems with cyber entities complying with foreign country laws
- Absence of supranational regulations: it is hard for LEA to access the users' data stored in the cloud in case of crime, severely limiting their capability to prosecute certain categories of crime
- Ransomware

Desired countermeasures:

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

Combining views of future scenarios

Different, **compatible** views can be combined into a **single** future scenario**.** **Incompatible** views (C and D in the example) lead to **alternative** scenarios.



Merging coherent, future views

The two views:

- **Social Networks**
- **Cloud Services**

are not contradictory, and are **complementary**.

They can be **merged** into a broader view, e.g.:

- **Personal Data Management**

Threats and defenses should be **revised** and **integrated** accordingly.

New threats may also emerge as a result of this fusion.

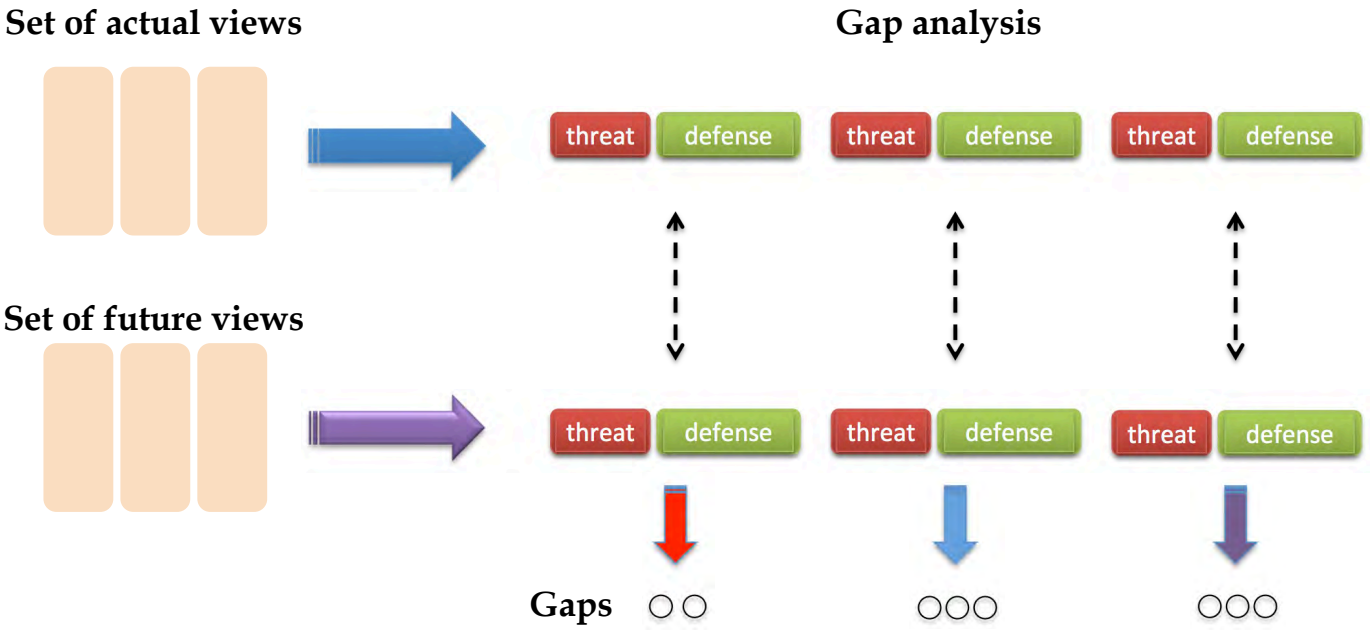
Gap Analysis (1/4)

Scenarios and views will be used in the subsequent **gap analysis** step.

- **GAP ANALYSIS:**
  the process of comparing actual and future views (i.e., the current knowledge and future needs) in order to identify **research gaps**

- **RESEARCH GAP:**
  a mismatch between a research subject related to a specific threat/ defence in the actual state and in a future view

Gap analysis (2/4)



Gap analysis (3/4): an example

Set of actual views

Gap analysis

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: 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

Template for gap analysis

Scenario title			
Threat	**Defenses (actual state)**	**Defenses (future view)**	**Research gaps**
Threat #1	…	…	…
…	…	…	…

Example of Gap Analysis (1/3)

GAP #	Views	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
1	Transportation Systems	Malware coming from the mobile device connected to the car infotaiment 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.	- Mobile anti-malware software - Network based Intrusion Detection Systems	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 WSNs that prevent non-authorized nodes to connect to the network and to send messages.	**Authentication in WSNs**
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**

Example of Gap Analysis (2/3)

GAP #	Views	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
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 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.	EU law enforcement has access only to 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.	An EU authority is established which is 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.	**Protection of the citizens' privacy**

Example of Gap Analysis (3/3)

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' rigth to privacy, which has to be considered as a fundamental right, is systematically infringed.

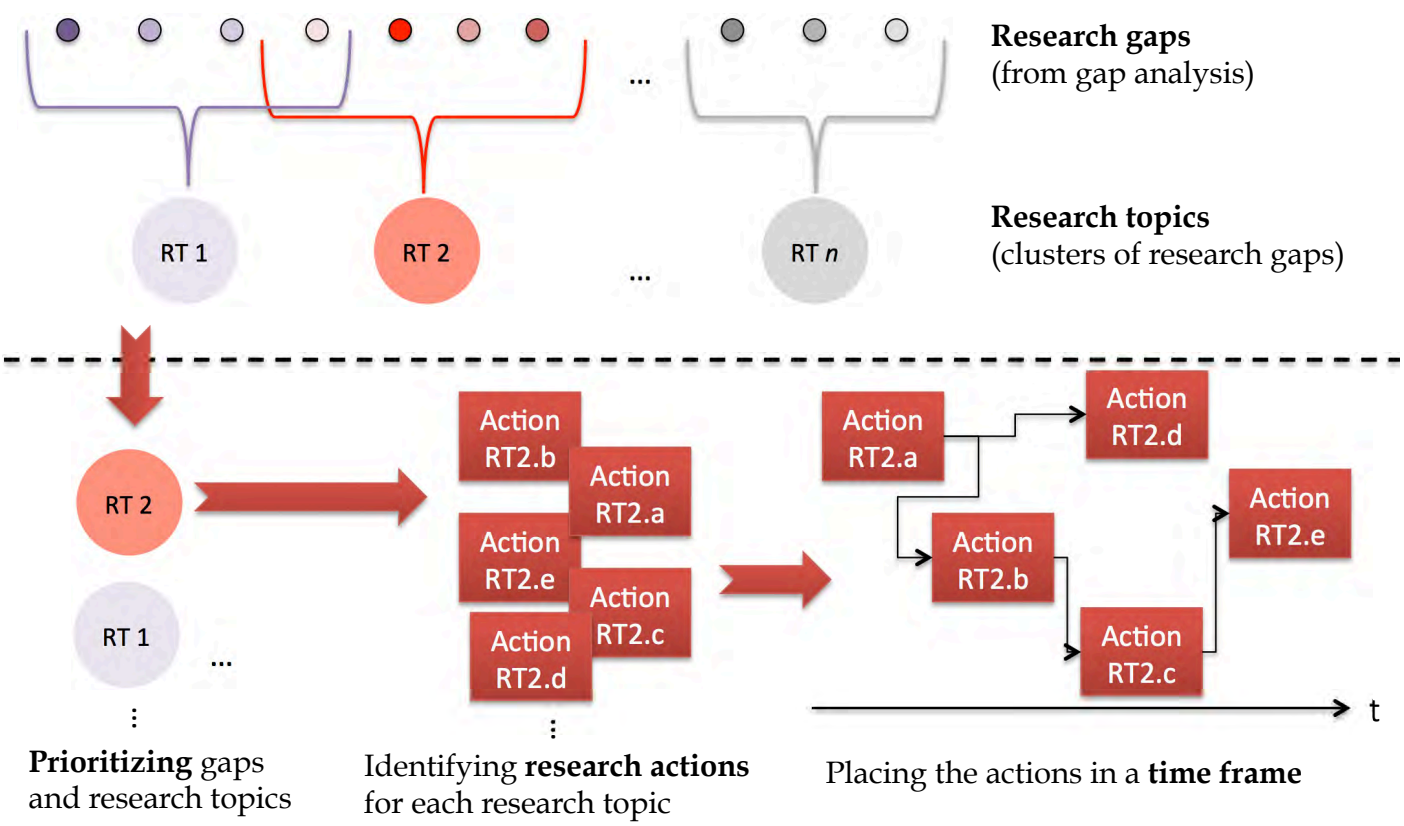
Roadmap construction (1/2)

Main steps:

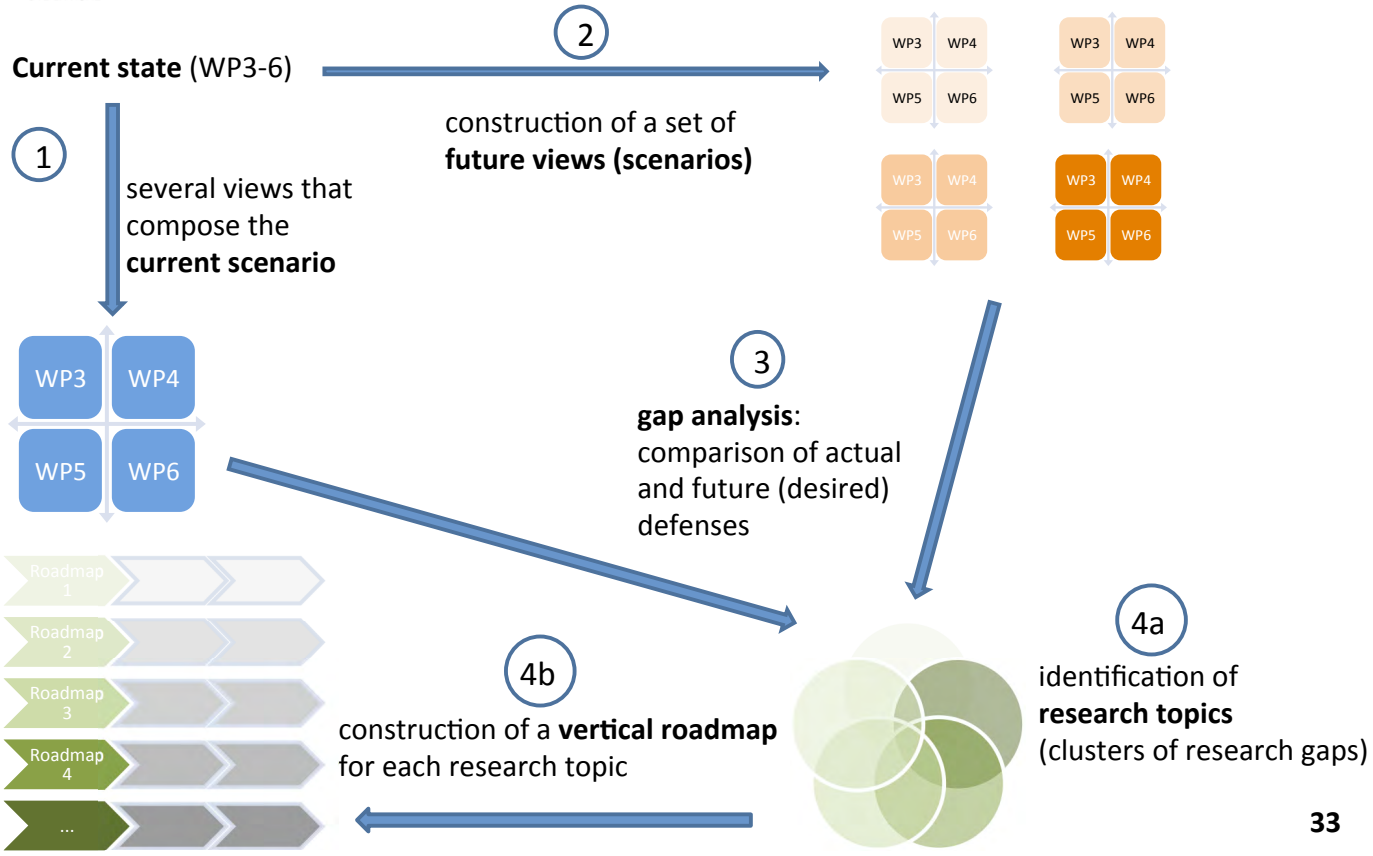
1. Defining a set of **research topics**: coherent clusters of related research gaps (possibly overlapping)
2. **Prioritizing** them using PROPRS' risk assessment methodology (Task 2.2)
3. Constructing a distinct **vertical roadmap** for each research topic: a collection of paths describing research **actions** required to address the research topic, to reach a given future objective
    1. identifying the **research actions** required to address a research topic
    2. putting the actions into a clear **time frame**, taking into account their interdependencies

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

Roadmap construction (2/2)



Summary of the roadmapping technique



Example of Roadmap Construction (1/5)

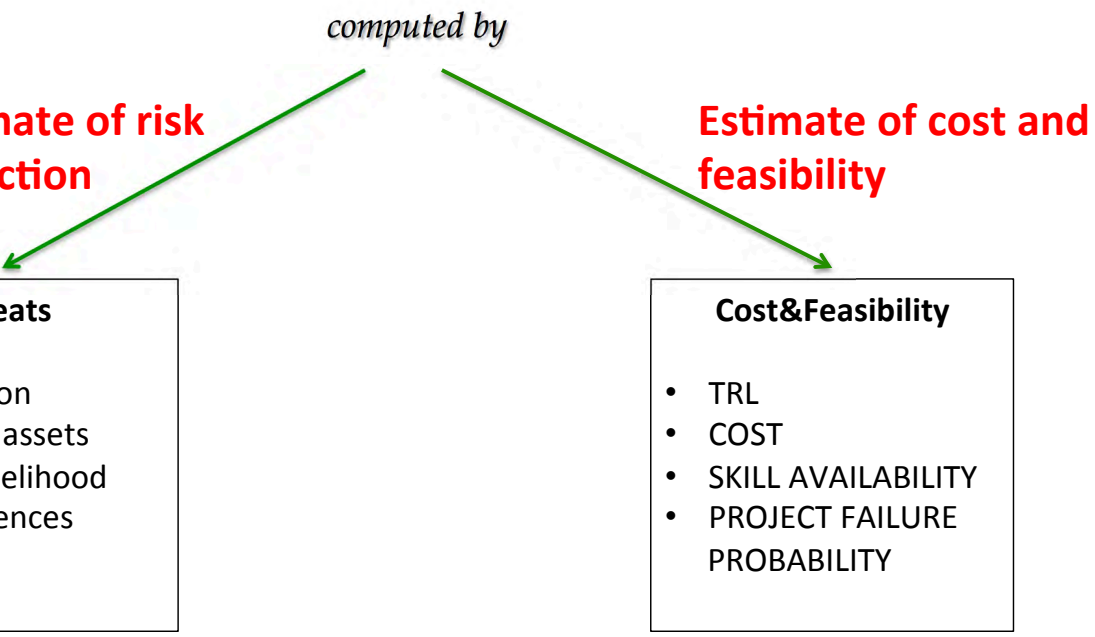
The previous research gaps can be **grouped** under two research topics:

- Topic #1: **Developing a Pan-European legal framework**
  - GAP #4 – Pan-European compliance
  - GAP #5 - Protection of the citizens privacy

- Topic #2: **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

➢ Research topics are **prioritized** using the Risk Assessment Ranking Methodology developed by PROPRS in D2.2.

Prioritizing research topics (D2.2)



Example of Roadmap Construction (2/5)

Research Topic #2	Title: Security of complex and unconventional systems
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.

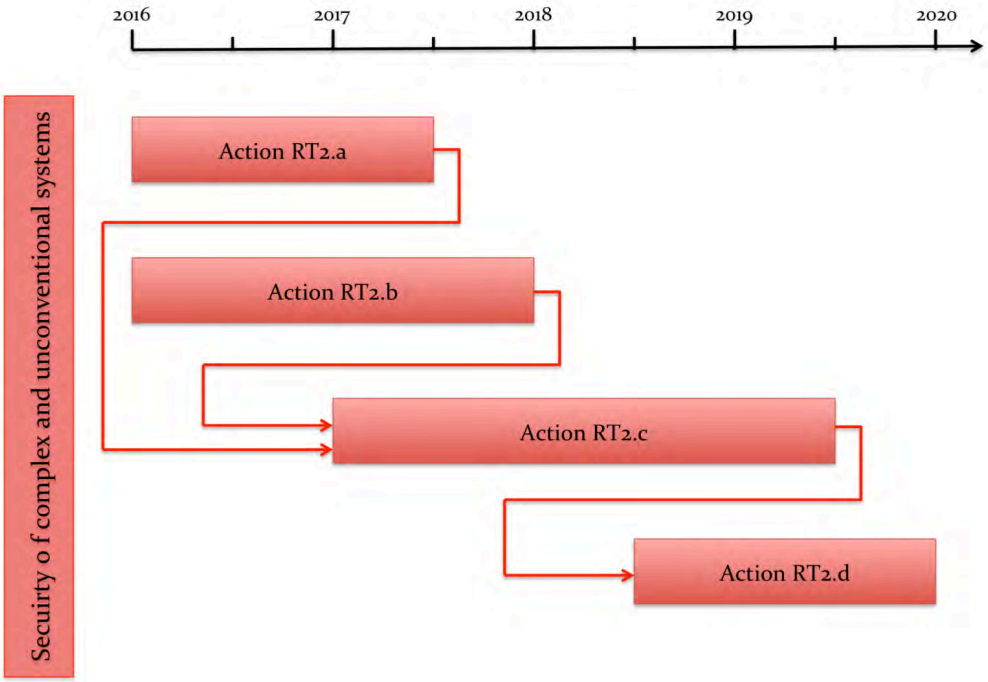
Example of Roadmap Construction (3/5)

Research Action #2.a	**Are the hardware platforms for embedded system suitable to run anti-malware solutions?** • **Do they have the required computational power?** • **What is the impact of an anti-malware solution on the energy consumption?**
	<u>Ranking information</u> Distance to the market: 5 Cost of the topic: 3 STREPs + 1 IP Availability of competences in Europe: 4
	Time span for addressing the action: 18 Months
	Actors: Research institutions, Industry
Research Action #2.b	Using biometric technologies to model users' behavior. • What is their degree of maturity? • Will wearable sensors be able to provide information to model users' behavior?
	<u>Ranking information</u> Distance to the market: 7 Cost of the topic: 4 STREPs + 2 IP Availability of competences in Europe: 5
	Time span for addressing the action: 24 Months
	Actors: Research institutions, Industry

Example of Roadmap Construction (4/5)

Research Action #2.c	**Do lightweight algorithms exist, capable to correlate information coming from different sources and to detect anomalies?**
	Ranking information Distance to the market: 4 Cost of the topic: 4 STREPs + 1 IP Availability of competences in Europe: 4
	Time span for addressing the action: 30 Months
	Actors: Research institutions
Research Action #2.d	• 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? • Shall the traditional architecture of computers and operating systems be drastically revised to make possibile the introduction of alternative and more reliable protection systems? • Shall the EC regulations be changed to ensure the trustwortiness of hardware and software components?
	Ranking information Distance to the market: 2 Cost of the topic: 8 STREPs Availability of competences in Europe: 3
	Actors: Research institutions, Industry, Policy-makers
	Time span for addressing the action: 18 Months

Example of Roadmap Construction (5/5)



Research roadmap for the topic 2: **Security of complex and unconventional systems**

References

- 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

- Wright, R.B. & Cairns, G., "Does the intuitive logics method – and its recent enhancements – produce "effective" scenarios?", *Technological Forecasting & Social Change* 80 (2013) 631–642

- Bradfield, R., Wright, G., Burt, G., Cairns, G. & Van Der Heijden, K., "The origins and evolution of scenario techniques in long range business planning", *Futures* 37 (2005) 795–812

CYBER ROAD

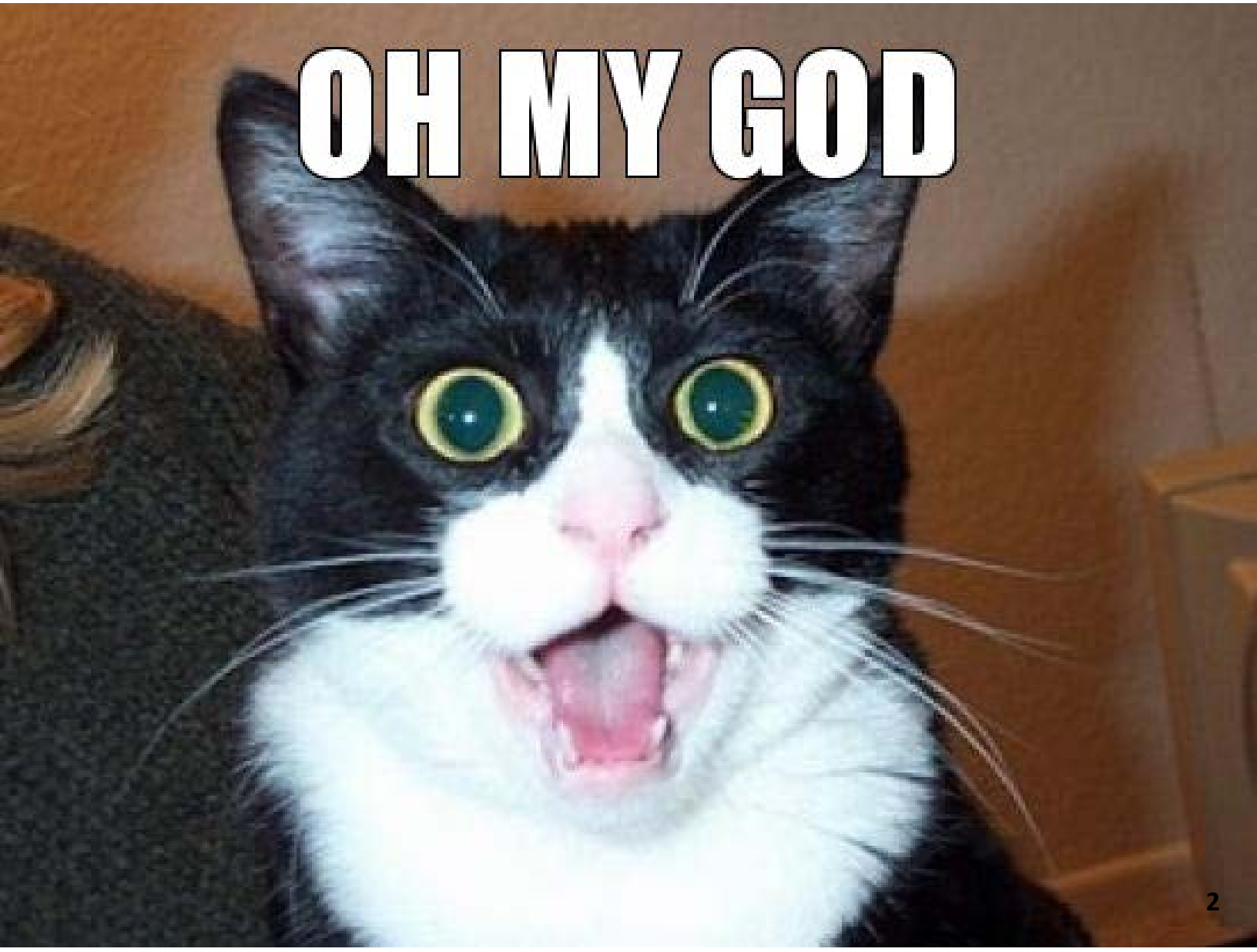
DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

CyberROAD roadmapping methodology EXAMPLE

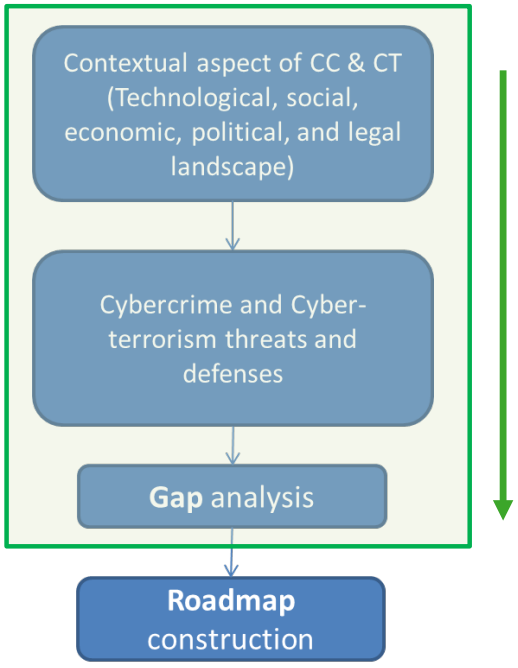
Darmstadt Meeting May 20-21, 2015

Version 1.0 – May 20, 2015
Responsible: Enrico Frumento (CEFRIEL)
Contributors: Federica Freschi (CEFRIEL)


OH MY GOD

Aim of this presentation

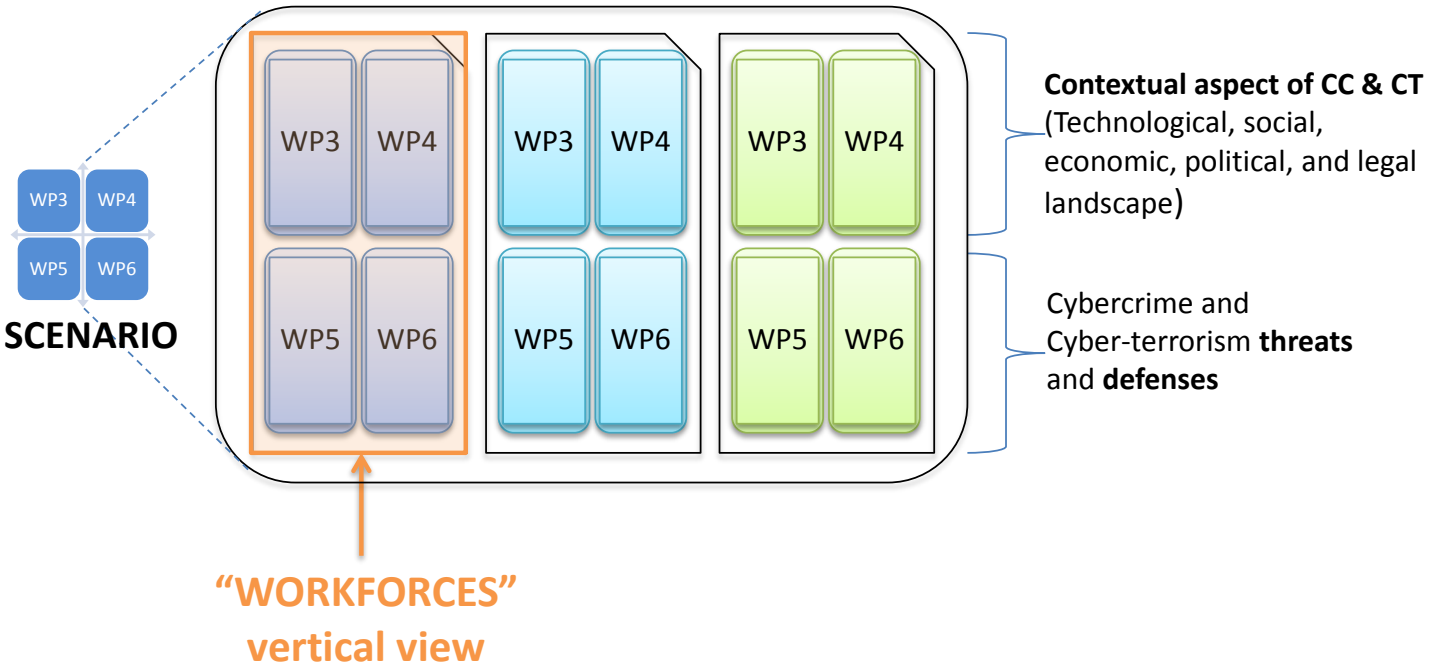
This presentation aims at providing an example of using the roadmapping methodology based on scenario analysis.



A concrete **example** will be shown in order to clarify the steps that from **scenarios description** lead to **gap analysis** following the process proposed by the methodology

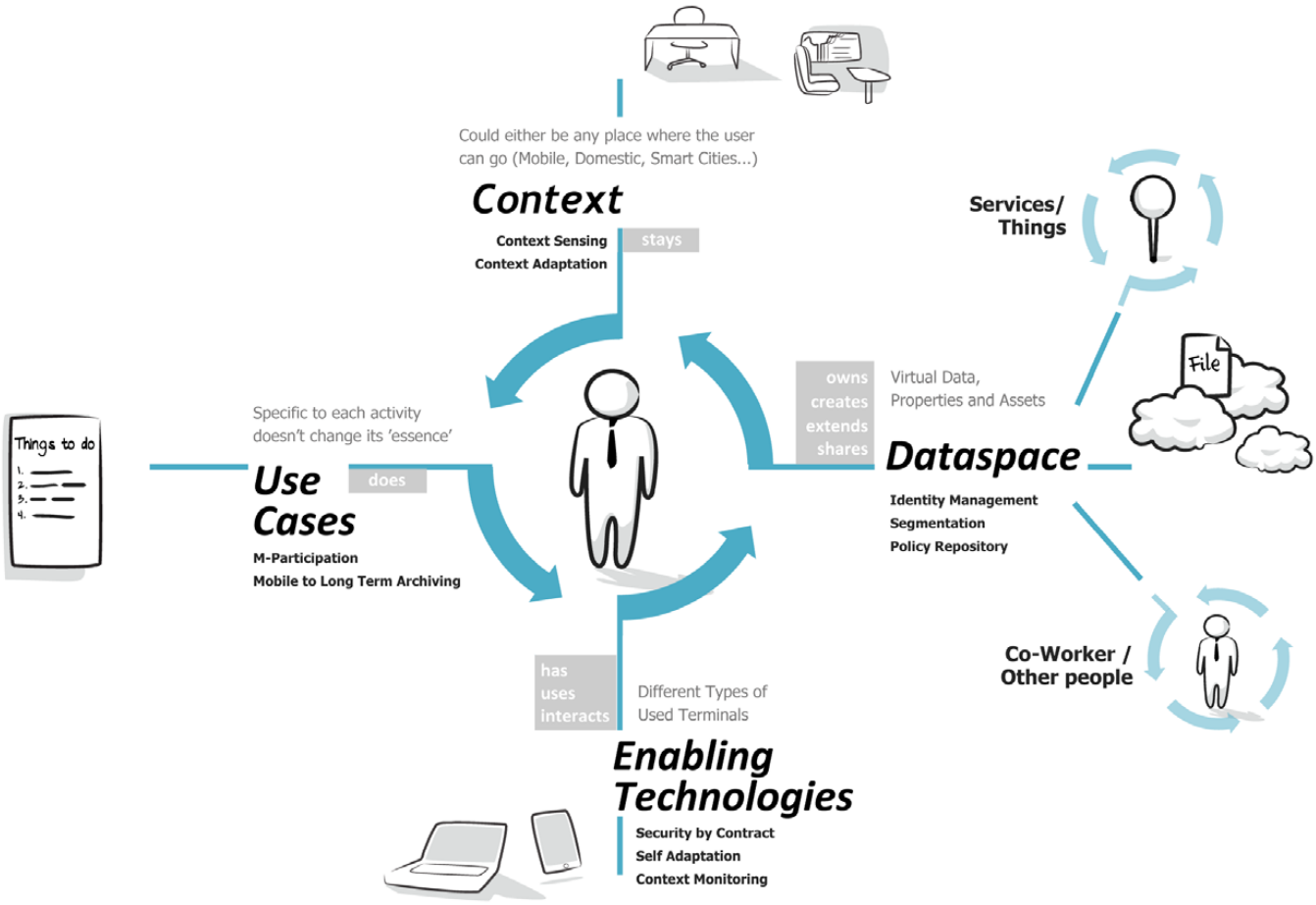
Some preliminary information (1)

- **For the scenario description, we started from the workforces evolution**

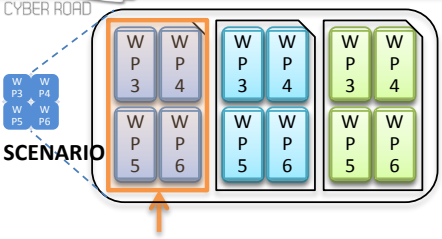


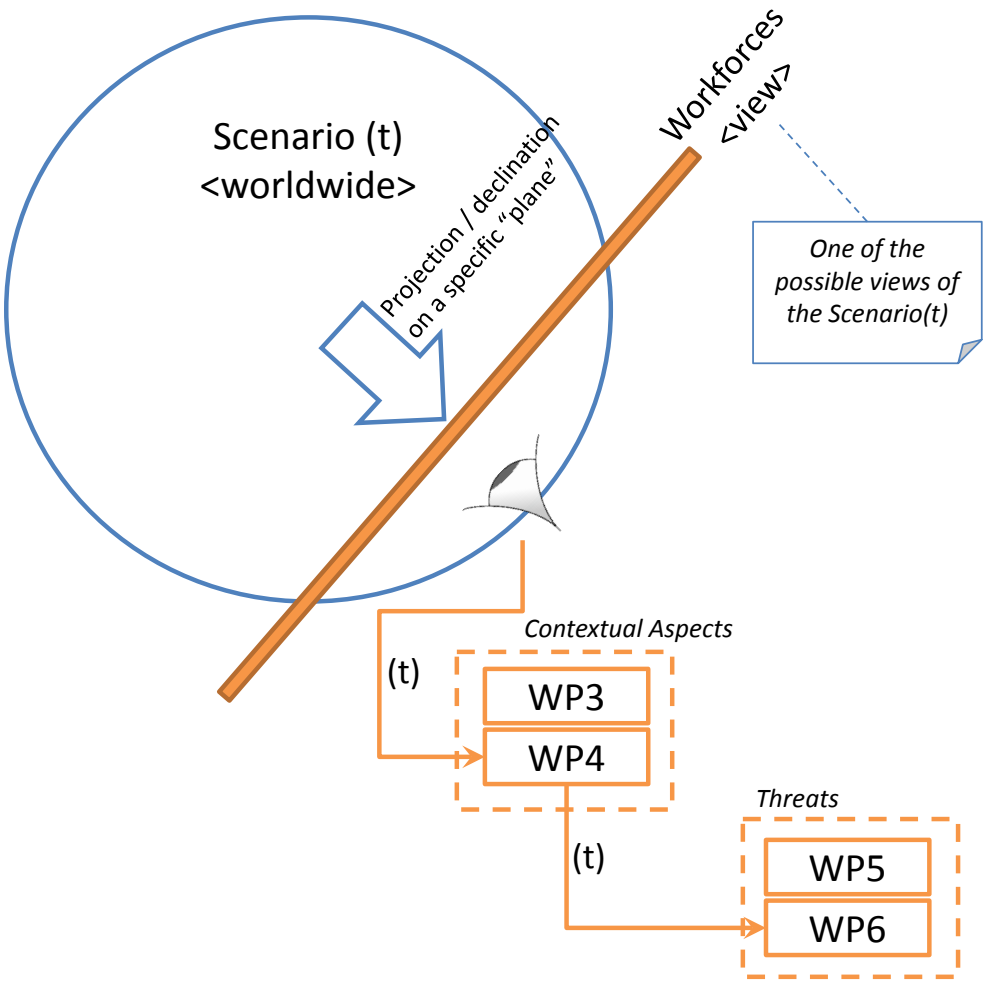
Some preliminary information (1)

- **Why workforces?? Presented @ the KoM as a leading view in CC**

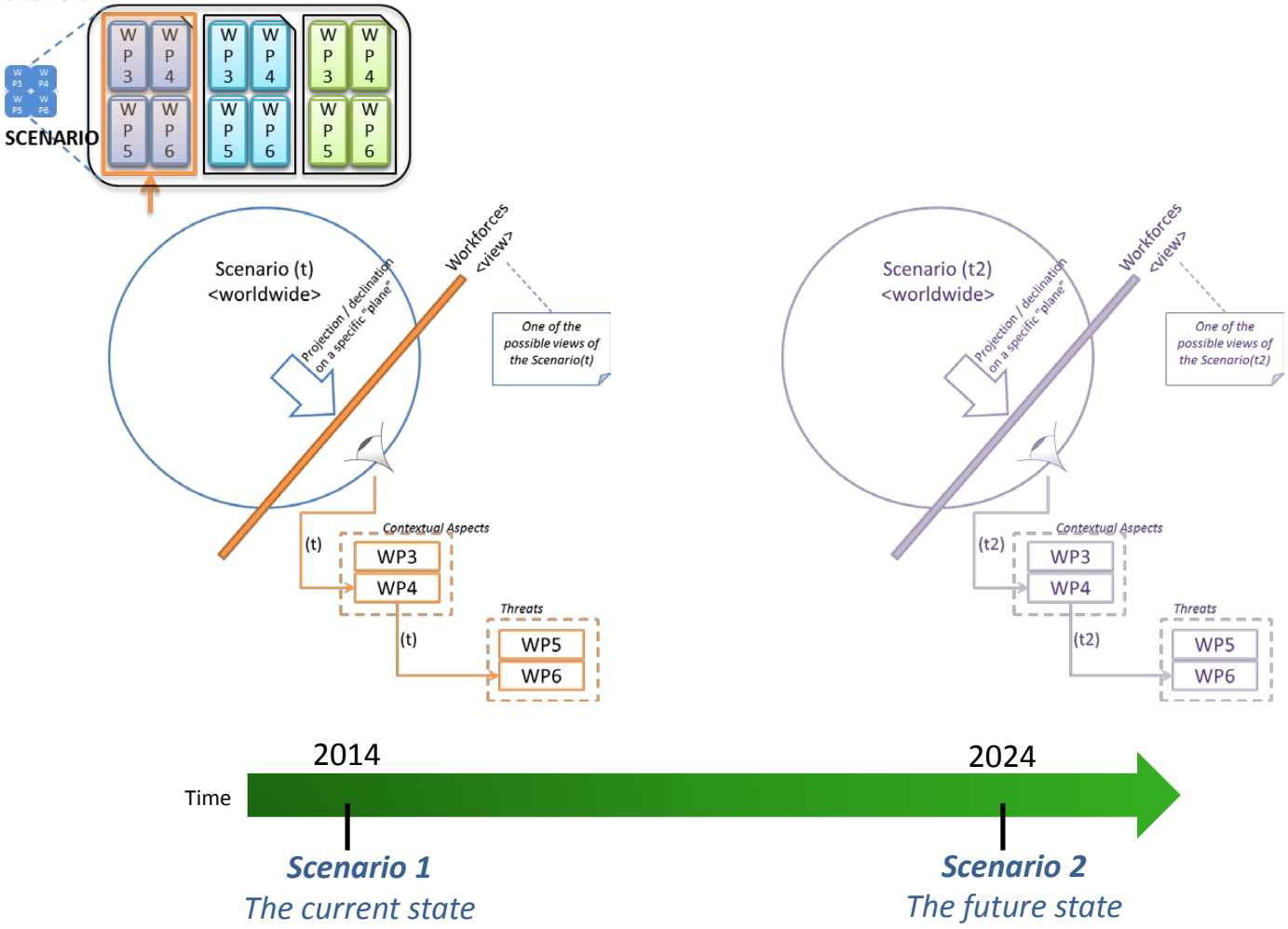


Aim of this presentation





Aim of this presentation

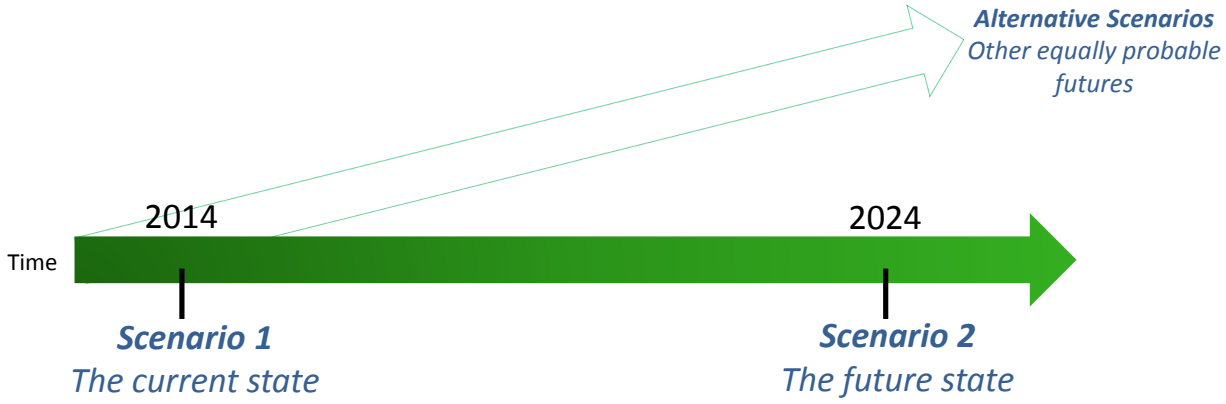


DO YOU REMEMBER DISSEMINATION PARK TOMORROWLAND?

SCENARIO (T1)

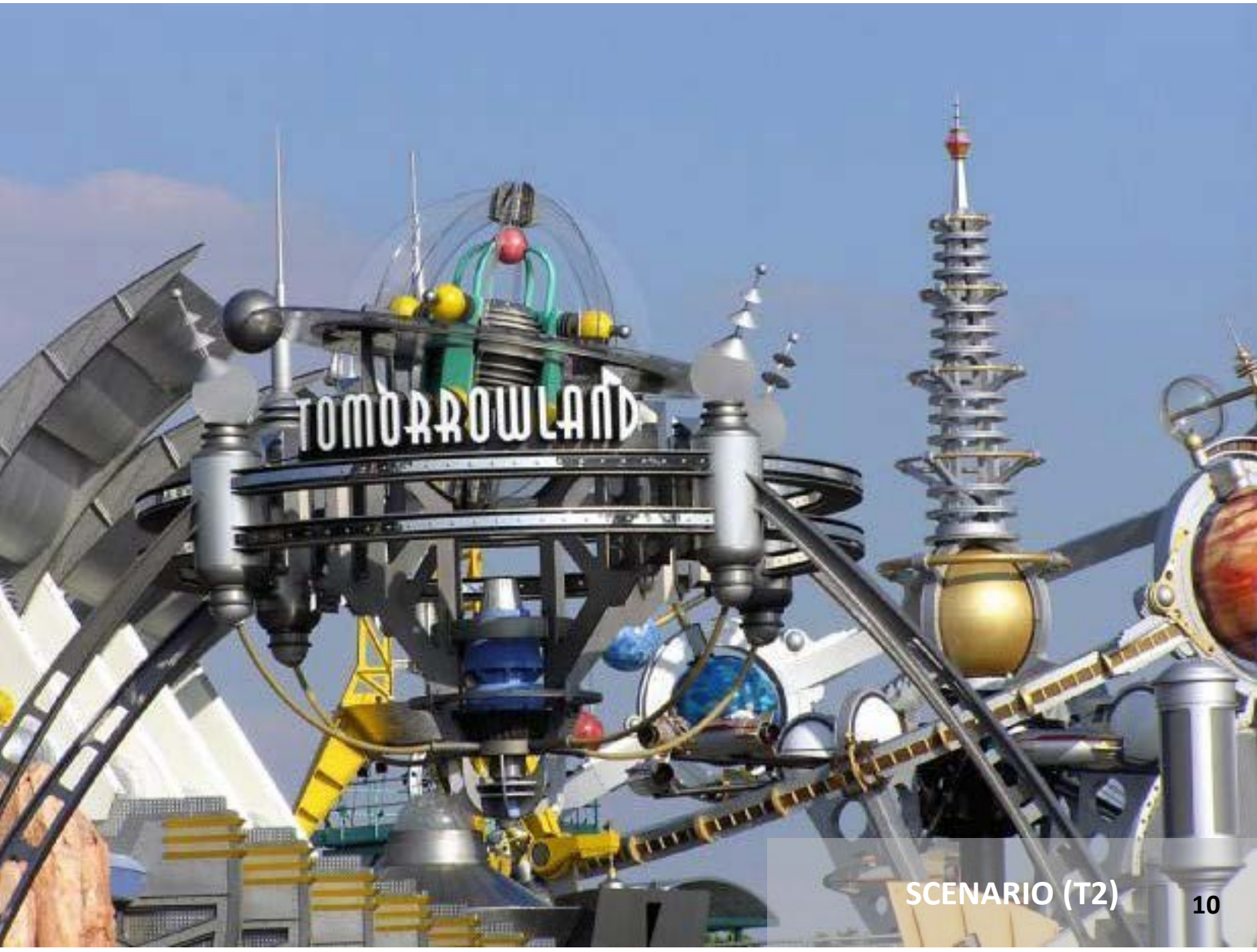
Some preliminary information (2)

- The description of the process is based on the comparison between **two different scenarios** temporally located in different periods



- The construction of these two scenarios, allows to analyse WORKFORCES topic from different perspectives: the current one and the future evolution
- Scenario is society ways of living today
- View is Workforces because it's a leading view

Source: "The Future of Identity Personal information space – The future of identities in a networked world", co-author E.Frumento, whitepaper, online at http://goo.gl/U6sH29 and in general any "futurology" whitepaper


TOMORROWLAND

.. ENTERING THE STAND OF WORFORCES


an experimental design demonstrating structural applications of plastics
HOUSE
OF THE
FUTURE
Disneyland
HOUSE OF
THE FUTURE
TOMORROWLAND

Views narrative description

View (t1) on workforces of Scenario (t1) - *Current state*

*Among the aspects, arising from the wide adoption of the mobile technologies there is the e**volution of the workforces**, i.e., the evolution of how the people are accustomed to work.*

*The digital devices have strongly shaped the way people are working and collaborating. **The everyday working activity can be seen as a continuous process of updating user's personal dataspace** through an enabling technology, selected among several with the usability in mind.*

*There is a **blending between private and professional** lives due to the flexibility to work at any time from different locations and consequently physical and virtual encounters seamlessly merge.*

*The **recent global recession** directly influences the labour market, adding new paradigms, **more flexibility and more mobility**. Thanks to **mobile and ubiquitous terminals**, a user could complete a task in any possible place, home, public spaces or company office. The market is constantly offering **new "methods" to access a user's own dataspace** like, for example, the expected revolution of the wearable electronic and IoT.*

***The essence of cybercrime is to abuse the trust chains** to steal assets. Within this scenario, what defines the security patterns are the trust chains, which are growing in number and are influenced by logical and physical contexts…*

View (t2) on workforces of Scenario (t2) - *Future state*

*This scenario sounds like a world **where individual rights are respected**, and where people profit from the services delivered by machines **without losing control over their personal information space**.*

*In a scenario where the integration of service largely uses a **peer-to-peer decentralized approach**, it is in general possible to have isolated service providers and isolated peers. Their business is to be disconnected from others for several reasons (privacy, independency, or hiding themselves from the others).*

***People are less dependent on one service provider**; interoperability is forcing services and platforms to compete in offering the best user experience. This kind of society has moves toward a complete **dematerialization of the personal dataspace on cloud services**. The public services (e.g., health) can exchange the data they need to deliver proactive personalized alerts and reminders. All these elements combine to create an idea of growing service customization.*

*Another important aspect to be considered in this scenario is the **revolution in automation field**, which implies the **diffusion of automatic transports**.*

Key drivers identification

Key drivers identification

	Current state	*Future state*
Blending Life	• NUI • Mobile terminals • Mobile workforces • Cloud • Payment system	• Immersed Human • Wearable/implantable • Mobile workforces++ • Federated cloud – Web 3.0 • Evolution of service provider including payment

Evolution of privacy & Identity	• New habits
	  • *Digital natives*
	• Low control of identities
	  • *Low perception of risks*
	• digital footprint
		• Redefined concept of identity & privacy
		• Full control of digital identities
		  • *Watchdogs*
		  • *Protected cyber humans*
		• New laws on privacy EU and new regulations
		  • *Less «hide between the cracks»*

View t1 (first part)

View t1: Current situation of Workforces

Summary (one page): *Among the aspects arising from the wide adoption of the mobile technologies there is the evolution of the workforces, i.e., the evolution of how the people are accustomed to work.*
The digital devices have strongly shaped the way people are working and collaborating. The everyday working activity can be seen as a continuous process of updating user's personal dataspace through an enabling technology, selected among several with the usability in mind…

Contextual environment

- **Society**: BLENDING LIFE: a world where physical and virtual encounters seamlessly merge. There is a Blending between private and professional lives due to the flexibility to work at any time from different locations. SOCIAL PLATFORMS: widespread distribution of social networking platforms. UBIQUITOUS workforces: user wants to complete a task in any possible place, home, public spaces or company office. USABILITY: To access the dataspace a worker can use several tools with different usability characteristics in order to accomplish easiness of use purpose.
- **Economic climate:** The recent global recession directly influences labor market adding new paradigms, more flexibility, more mobility
- **Legal and Law enforcement issues:** Privacy and data legislation is important to help defining which data of the personal dataspace a user can access, in a specific place to protect his identity, privacy or to respect some security policies. Relevance of the Cybersecurity insurance and connection with the active defense systems

Technology & (technology enabled) services (WP4)

- **ICT available**: widespread use of mobile devices to perform working activities, New interfaces: the market is constantly offering new "methods" to access a user's own dataspace, diffused online payment systems in every environment
- **Services**: machines collect personal data from users who want to have access to services. Users want to use those services and are therefore willing to give away personal data, following a data-for-(free)services logic. New Dataspace services: moving toward a complete dematerialization of the personal dataspace on centralized cloud services

Cybercrime & Cyberterrorism specific issues (WP5 and WP6)

- **Offensive technologies**: Increased importance of the human element in the enterprise processes , Heterogeneous attack surface for the enterprises/private users Cybercrime market and cybercrime as a service (Cybercrime=marketing), Legislation inconsistencies (hide between the cracks)
- **Defensive technologies:** Privacy and data legislation is important to help defining which data of the personal dataspace a user can access, in a specific place to protect his identity, privacy or to respect some security policies - Relevance of the Cybersecurity insurance and connection with the active defence systems. New authentication methods (no password, behavioural, fuzzy security, ...) - New counterattack and prevention technologies - Inclusion of human elements inside an holistic strategy of protection

Possible key driving factors: Blending life, Evolution of privacy & Identity

NEXT SLIDE

Threats and Defences Details – View t1

Threats

- Increased importance of the human element in the enterprise processes
- Heterogeneous attack surface for the enterprises/private users
- Cybercrime market and cybercrime as a service (Cybercrime=marketing)
- Legislation inconsistencies (hide between the cracks)

Defences

- Legal and Law Enforcement issues:
  - Privacy and data legislation is important to help defining which data of the personal dataspace a user can access, in a specific place to protect his identity, privacy or to respect some security policies.
  - Relevance of the Cybersecurity insurance and connection with the active defence systems.
- Technological issues:
  - New authentication methods (no password, behavioural, fuzzy security, ...)
  - New counterattack and prevention technologies
  - Inclusion of human elements inside an holistic strategy of protection

Threats		**Desirable countermeasures**
Threat 1	Threat description	Desirable countermeasures for threat 1
	Assets targeted by the threat	
	Threat likelihood	
	Consequences of the threat	
...	...	...

View t2 (first part)

View t2: Current situation of Workforces

Summary (one page): *In a scenario where the integration of service largely uses a peer-to-peer decentralized approach, it is in general possible to have isolated service providers and isolated peers. Their business is to be disconnected from others for several reasons (privacy, independency, or hiding themselves from the others)…*

Contextual environment

- **Society**: IMMERSED HUMAN: humans are surrounded constantly by a technological environment in every aspect of their life. Persistent interference by the service providers in providing suggestions (covering every sphere of life) in line with the person profile
- SOCIAL PLATFORMS: widespread distribution of social networking platforms: the trend is oriented to more decentralized networks. UBIQUITOUS workforces: user wants to complete a task in any possible place, home, public spaces or company office.
- **Economic climate:** Some networks even take money for their event stream, e.g., because they host all the stars and celebrities. Government have a great interest in influencing future policies
- **Legal and Law enforcement issues:** term-of-service (ToS) are becoming more invasive and start to regulate more aspects of cyber lives than in the past. The users accepting them automatically comply to these set of "rules". Cross-border legal problems with cyber entities complying with laws frameworks of a foreign country. Right to be forgotten evolved into something functional (see the book Delete di Viktor Mayer Shörimberger)

Technology & (technology enabled) services (WP4)

- **ICT available**: New interfaces: wearable revolution and IoT. New Dataspace services: Moving toward a complete dematerialization of the personal dataspace on cloud services. Federated cloud where there are common standards for both hardware and software companies. Big Data: it is possible to use repositories of social and transactional data, collectively known as the "digital commons." Purchasing habits, media consumption, and travel plans are all retrievable on these commons (Data are all anonymized). Large (high Kb/s) and long bandwidth (long lasting connections)
- **Services**: Digital ecosystem: Community of people who interact, exchange information, combine, evolving in terms of knowledge, skills, contacts, in order to improve their lives and meet their needs.. Revolution in automation field: Widespread use of automatic transports (e.g., electric cars). Widespread use of mobile devices to perform working activities (Mobile Workforces++)

Cybercrime & Cyberterrorism specific issues (WP5 and WP6)

- **Offensive technologies**: New forms of abuses/new targets (Human, IoT, Infrastructure, linked open data, social, connected things…). Minor perception of information security risk because of people, finding themselves living in blending life, starts to take for granted the technological infrastructure and it becomes somehow "transparent" to the user. Wide adoption of authentication behavioral methods and behavior theft (like nowadays the identity theft). Abuse of unnoticed trust chains also due to the increasing of disappearing computing or immersed human paradigms. Extreme data broker, i.e. fake identity trading.
- **Defensive technologies:** Policies related to privacy are becoming less cumbersome, the central government establish the general directions and criteria. Cross-border legal problems with cyber entities complying with laws frameworks of a foreign country. Right to be forgotten evolved into something functional (see the book Delete, Viktor Mayer Shörimberger). Situational security authentication system (based on behaviour of humans and machines)

NEXT SLIDE

Threats and Defences identification – View t2

Threats

- New forms of abuses/new targets (Human, IoT, Infrastructure, linked open data, social, connected things…) [2]
- Minor perception of information security risk because of people, finding themselves living in blending life, starts to take for granted the technological infrastructure and it becomes somehow "transparent" to the user [1,2,5]
- Wide adoption of authentication behavioural methods and behaviour theft (like nowadays the identity theft)[1]
- Abuse of unnoticed trust chains also due to the increasing of disappearing computing or immersed human paradigms[2]
- Extreme data broker, i.e. fake identity trading [3]

Defence

Legal and Law Enforcement issues:

- Policies related to privacy are becoming less cumbersome, the central government establish the general directions and criteria
- Term-of-service (ToS) are becoming more invasive and start to regulate more aspects of cyber lives than in the past. The users accepting them automatically comply to these set of "rules"
- Cross-border legal problems with cyber entities complying with laws frameworks of a foreign country.
- Right to be forgotten evolved into something functional (see the book *Delete*, Viktor Mayer Shörimberger)

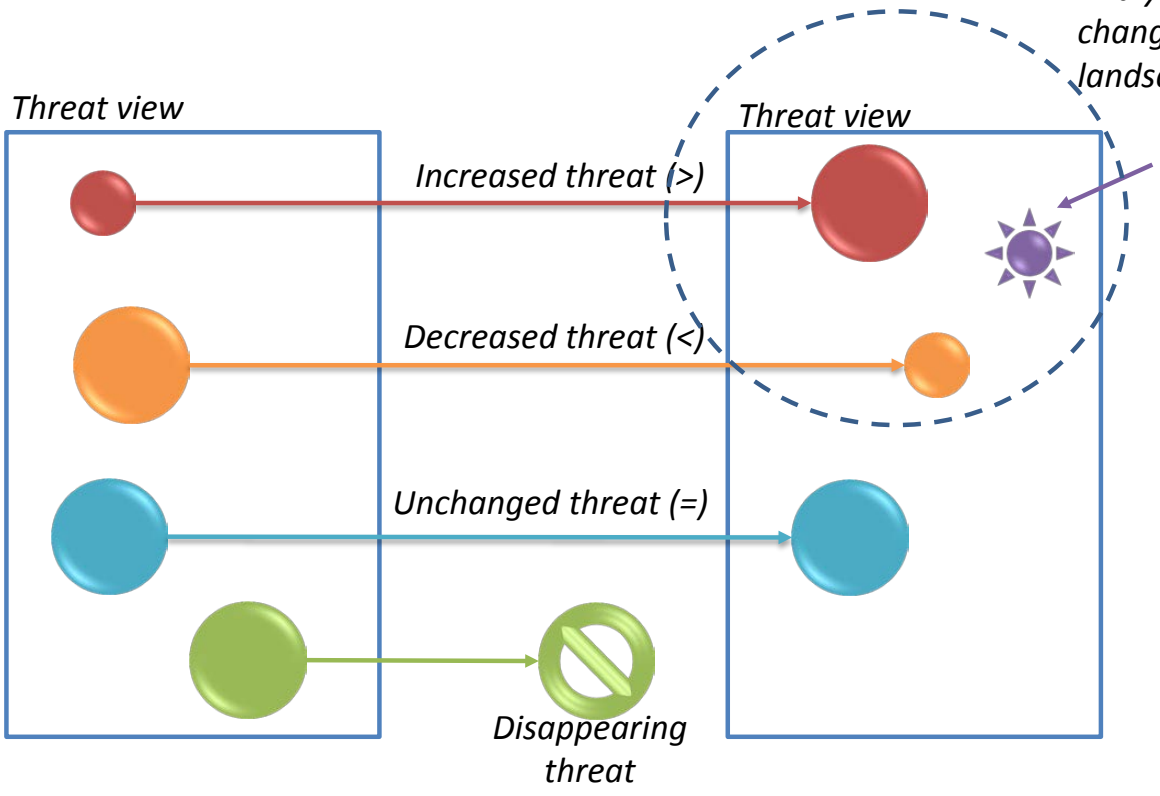
New protection systems

- Situational security authentication system (based on behaviour of humans and machines)
- Protection systems that emulate humans as human honeypot. Personality

Threats		**Desirable countermeasures**
Threat 1	Threat description	Desirable countermeasures for threat 1
	Assets targeted by the threat	
	Threat likelihood	
	Consequences of the threat	
…	…	…

Threats and Defences identification – View t2

The aim of GAP Analysis is to track the changes in the threat landscape



t1 → t2

Threats and Defences identification – View t2

- **A properly cooked research gap is made of different ingredients:**
  - Understand the Initial (t1) and final (t2) situations
  - The path which connects t1 and t2
    - Directions of the ongoing research and an estimation of how this will contribute to fill the gap @ t2
  - How threats will evolve between t1 and t2: increased, decreased, equal, disappeared or new-born threats
  - Clustering of gaps emerging from the different Views
    - Manually done and reviewed by "grouped" experts into the project
    - Possible description using some sort of threat modelling languages (e.g. SDL Threat modelling language)
    - Discuss if the process catches all the foreseen threats
  - Integrate Gaps already identified from Deliverables that are still missing

Gap Analysis

GAP #	Status	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
1	>	Abuses on new targets (Human, IoT, Infrastructure, linked open data, social, connected things…)	Statistics and detection of preferred attacks patterns	Threat intelligence and detection of new opportunities before they are exploited; emulate human behaviour and creation of "human honey pots"	Threat and attack intelligence, attack simulation infrastructures
2	>	Change in perception of information security risk because of people living in blending lives, differently realize that their assets are stolen and take for granted the technological protection infrastructure; technologies are "immersed"	Awareness programs to train people on risks of online lives	Improved awareness methodologies for citizens; security by design; law protecting e-citizen against "bad" design	Law, new awareness methodologies with a "human touch"
3	>	Wide adoption of authentication behavioural methods and behaviour theft (like nowadays the identity theft)	The behavioural security is a new paradigm not still on the market	Situational security authentication system based on behavioural of humans + machines; fuzzy authentication methods	Behavioural security
4	=	Abuse of unnoticed trust chains also due to the increasing of disappearing computing or immersed human paradigms	Identification of trust chains; extended testing; arm race with attackers in finding exploits	Identification of NEW trust chains before attackers with proper testing and developing CMMs	Automated ways to identify existing trust chains, increasing of threat management models
5	>	Extreme data broker, i.e. fake identity trading	Data broker back market is in its infancy	Increased exchange of data coming from the different targets, improved trading systems	Improvement of the monitoring tools of CC markets
	>	Increased importance of the human element in the enterprise processes	Evaluation of risk introduced by the human element; awareness for mitigation	Right to be forgotten; automatic risk evaluation of human related threat, improved automatic psychological profiling	Better integration of human sciences (psychology and sociology) into security
	<	Legislation inconsistencies	New EU data privacy law	Policy related to privacy is less cumbersome; the central government establishes the central directions and criteria	More EU harmonization; problems with non-EU entities handling EU data

GAP #	Status	Threat (future view)	Defense (actual view)	Defense (future view)	Research gap
1	!	Term-of-service (ToS) are becoming more invasive	NA	Market is becoming extremely aggressive in terms of what it can be done with released data	Monitor the ethical and legislative infrastructure for the ToS of non-EU entities.
2	!	Implantable terminals	NA	Evolution of implantable terminals and in general the appearance of the immersed human paradigm completely erase the explicit interfaces of devices	New ways to alert users of ongoing attacks or increased risks