Funded by the European Commission

Seventh Framework Programme

CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D 7.8 Second ARES-Workshop Report

Internal Project Workshop

Date of deliverable: 31/12/2016
Actual submission date: 02/04/2016

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 0.0

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	01/01/2016	SBA
0.2	Revision	01/03/2016	NCSRD/SM
0.1	Revision	01/04/2016	UNICA
1.0	Final draft	02/04/2016	SBA/UNICA

D7.7
First Workshop Report

Responsible
Peter Kieseberg (SBA)

Contributor(s)
Davide Ariu (UNICA)
Elisa Constante (SM)
Peter Kieseberg (SBA)
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. The main aim of CyberROAD, besides aligning law enforcement agencies (LEAs) with research institutions and other major players throughout Europe, lies in the development of a comprehensive research roadmap, which will enumerate current research gaps and anticipate emerging threats.

In order to foster development of the roadmap, specific application areas need to be defined that cater for the need to provide attack and gap analysis in practical applications. In order to discuss the needed research directions, an internal project workshop was organized within the consortium. The target of this Workshop was the specification of fundamental scenarios in order to build a fundament for further development of the research topics. These discussions inside this workshop were based on the research progress derived from the first FCCT-Workshop that was collocated with the ARES conference in August 2015 in Toulouse. This guarantees that a lot of external input could be incorporated into the results of this Workshop, while generating the scenarios in a fast and efficient way. Furthermore, holding this Workshop as an internal venue allowed very critical reflection on these inputs and learnings, while analysing the further work without need to cater for external persons, e.g. with regards to confidentiality.

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 research 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 the activities in the second ARES-Workshop that was conducted in Vienna on December 9th 2015 as a follow-up event to the first FCCT, the "First International Workshop on Future Scenarios for CyberCrime and CyberTerrorism".

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

- Align the results that have been gathered by the project consortium,
- Incorporate feedback received by the public and the professional communities,
- Organize and speed-up the project progress and give concise targets for the partners,
- Enhance direct communication with the general public.

The activities targeted the following communities:

a) **The general public:** While this workshop was mainly held within the consortium, it contained a valuable wrap-up and lessons-learned of the previous public workshops that targeted raising awareness on the issue of emerging Cyber Crime and Cyber Terrorism threats among the general public.

b) **The scientific community:** During this Workshop, the continuation of the FCCT that was started within the CyberRoad-project was discussed and new relevant partners were identified.

c) **The potential stakeholders and policy makers:** The identification of new stakeholders on the governmental, as well as the private sector is of the utmost importance in order to generate a practical roadmap that is based on the actual state of the world, not only research-wise, but also with respect to the legal and organizational aspects of the European landscape in the area of research on Cybercrime and Cyberterrorism. This workshop included discussions on the changes in the European landscape throughout the last year of the project duration, as well as the expected changes within the next years.

1.3 STRUCTURE OF THIS DOCUMENT

This document is structured as follows:

- **Chapter 1** provides an introduction and the context of the two workshop activities
- **Chapters 2 & 3** are related to the Workshop on scenario building that took place in Vienna in December 2015, with Chapter 2 detailling the workshop aims and Chapter 3 the results on actual scenario building.
- **Chapters 4 & 5** are related to the joint Workshop with the sister project Carmino and Courage that was held in March 2016 in order to generate a common roadmap.
- **Chapter 6** contains all the appendices.

2.1 AIMS FOR SCENARIO BUILDING

Scenario building is one of the major targets of the Cyberroad project that is directly derived from the roadmapping methodology that was developed within this project: Based on the scenarios, threats and attack vectors are generated that, together with the state of the art in detection and mitigation, serve as a basis for the gap analysis that results in the roadmap on research needed in order to overcome the implications of these gaps. Furthermore, practical scenarios not only allow for a concise gap analysis, they also guarantee that the gaps identified are related to actual civilian and governmental, as well as industrial needs and allow simple rating and grading based on their relevance to certain major players in the field. Furthermore, the development of scenarios not only allows the generation of a practical roadmap, it also allows good illustration of the results to the general, as well as the informed, public, as the practical effects are not hidden behind abstract research questions, but directly visible together with their practical implications. This is also very important in order to legitimate the efforts spent within the project towards the European citizens and member countries.

The main aims of the second ARES-Workshop that took place on December 9th 2015 in Vienna at SBAs premises were the following:

1. Collection and concentration of recent research results, mainly derived from the First International Workshop on Future Scenarios for CyberCrime and CyberTerrorism (FCCT) that was organized by the CyberRoad project in conjunction with the 10th ARES-conference in Toulouse in August 2015.
2. Development of a set of fundamental scenarios that on the one side provide a good coverage of the fields identified as relevant for the project scope and on the other hand does not produce too much overlap between the single scenarios. This goes hand in hand with the preparation of a strategy for the actual preparation of these scenarios and the resulting views (see the document on the research and roadmapping methodology).
3. The definition of a strategy for the preparation of the final research roadmap, especially considering coordination with the projects CAMINO and COURAGE in order to achieve a consolidated view and a consolidated roadmap that can be utilized for future research endeavors.
4. The definition of actions for communication and dissemination for the final project results and during the last 5 months of the project duration.

2.2 WORKSHOP PARTICIPANTS

Since the Workshop was heavily focused on scenario building and on the definition of the fundamental scenarios, as well as planning a strategy for the development of the actual scenarios, views and the gap analysis, the attending partners mainly represent a selection of those partners that are heavily active in this topic of the project. In order to keep the meeting lean and small, only a selection of the partners was present:

- UNICA (Project Coordination)

- NASK (Leader T5.4 Cybercrime Research Topics)
- SM (Leader T5.4 Cybercrime Research Topics)
- CEFRIEL (Leader T2.4 Cybersecurity Research Roadmap Generation)
- SUPSI (Leader WP2)
- NCSRD (Leader WP7)
- SBA (Workshop Organizer)

3 PREPARATION OF THE CYBERCRIME AND CYBERTERRORISM SCENARIOS

At the Workshop in Vienna, various decisions were made not only concerning the actual work inside the project, but also the alignment with the projects CAMINO and COURAGE and the positioning of CyberRoad within the research environment. In addition, a clear and concise plan for the development of the fundamental scenarios, the respective views and of the final roadmap during the last 5 months was generated. This also included an analysis on the state of the project by the project coordination, including the state of all deliverables and their readiness for final reporting.

3.1 SELECTED SCENARIOS AND VIEWS

With respect to the research and scenario development methodology that was proposed during the project, each scenario is split into different views that can be developed by different partners independently. Based on an initial proposal by the task coordinators, a structure for the scenarios and views was developed at the workshop. It was also decided that, in order to reduce overlap and double efforts for analyzing the current state of the art and the development of views that fall into both categories, the categories of cybercrime and cyberterrorism are not split between the partners, i.e. a partner working on a specific view will do this for both categories. It was therefore also decided to consider the tasks T3.3, T5.4 and T6.5 as one single “super-task” producing one single document containing the CyberROAD scenarios and research topics. If needed, the document can be split into three deliverables at the end of the project.

While the deliverable will be proposed in the form of one deliverable derived from a super-task, still each of the three original tasks shall propose own scenarios based on practical results, evidence and results collected within the past deliverables of the respective task. In addition, this new structure gives the opportunity to work together more closely by enriching the scenarios proposed by the other original tasks and adding alternative perspectives. This can be summarized as

- Helping to identify original views
- Helping to enrich the context of the existing views
- Helping to identify threats against the existing views
- Helping to identify countermeasures for the existing views
- In general providing new perspectives and helping to enrich.

The table shown in the following page, gives an overview on the selected scenarios and on the views.

The main discussions at the Workshop revolved around the definition and especially the differentiation of the scenarios and views in order to avoid overlaps, as well as gaps, between the scenarios and views.

Scenario	View	Partner
Social Sharing	(i) Social Network (CC and CT)	NASK & FORTH
	(ii) Life logging (CC and CT)	RHUL
	(iii)Wearable device (CC & CT)	SUPSI
Building Automation	(i) Smart Building and domotics	SBA
Energy	(i) Water Utilities	SM
	(ii) Gas Utilities	VITRO
	(iii) Smart Grid	VITRO
Transportation	(i) ICT Systems for Transportation	NCSRDD
	(ii) Aviation	NCSRDD
	(iii) Smart Roads	NCSRDD
Healthcare	(i) Mobile Health and Augmented Humans	CEFRIEL
	(ii) Hospital 2.0	CEFRIEL
	(iii) P4 Medicine	SBA
Security and safety	(i) Fighting Cybercrime as a Service	CDF
	(ii) Attribution of cyber crime	NASK
	(iii) Trusted Components (SW and HW, supply chain)	TUD
Workforce	(i) Enterprise 2.0 (BYOD, ubiquitous connectivity)	CEFRIEL
Industry	(i) Industry 4.0	SM
	(ii) Just in time production	TUD
Financial Services	(i) Cryptocurrencies	CDF
	(ii) Online Banking	RHUL
Data Driven Economy	(i) Big Data (CC and CT)	SBA
	(ii) Control over data (includes privacy, data protection and leakage, OS/computer system logging, Software as a Service (SaS))	SBA

Table 1 – Scenarios and Views

3.2 *VIEW DOCUMENT STRUCTURE*

At the Workshop, a proposal for the document structure for the views that need to be filled by the partners was proposed by the task coordinators and discussed by the participants. Having a structured approach based on a common document structure was discussed and considered to be very important in order to enhance the speed of the project development and to guarantee the possibility of aligning the views in order to generate one single final roadmap.

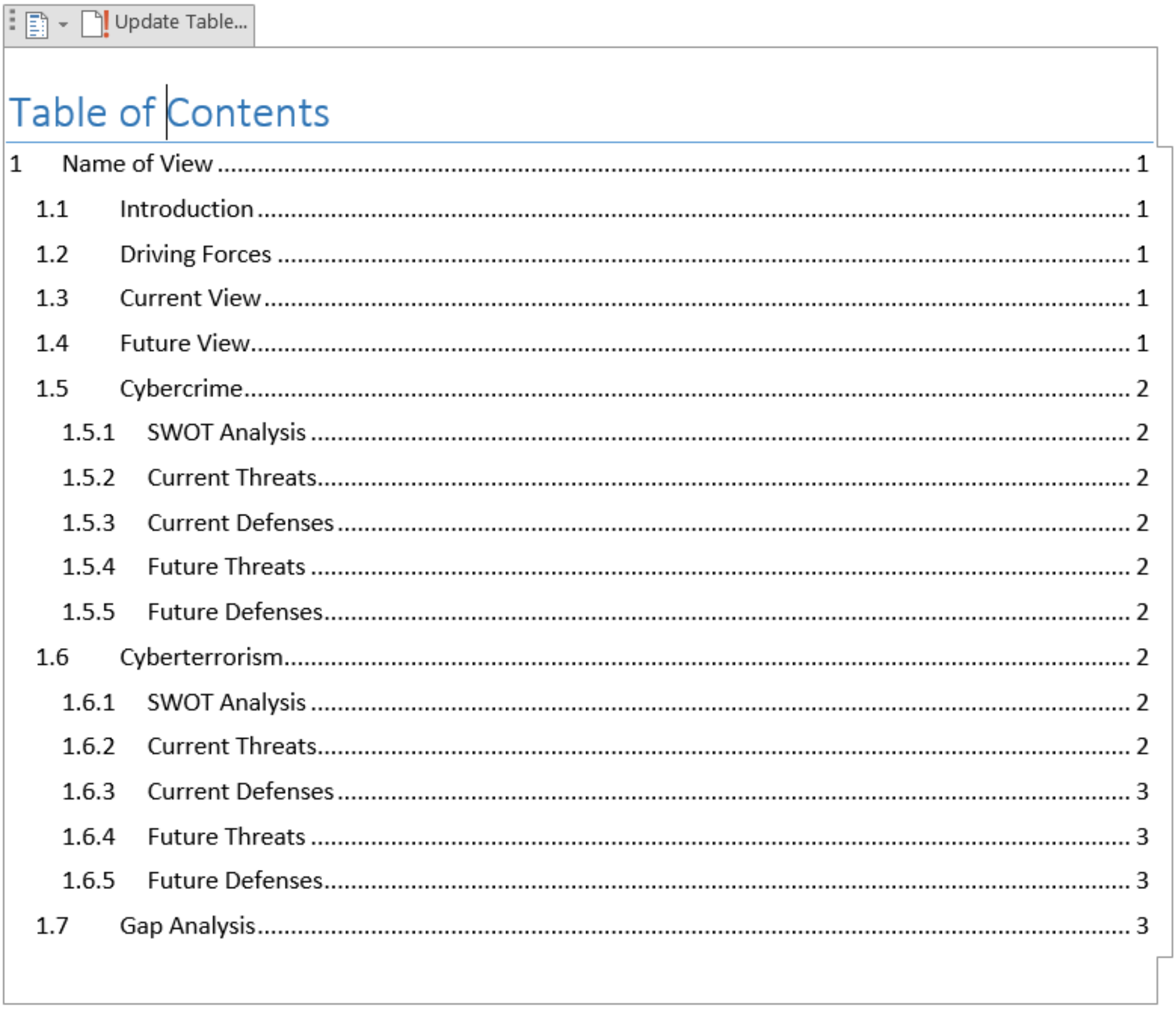


Table of Contents

1 Name of View 1
1.1 Introduction 1
1.2 Driving Forces 1
1.3 Current View 1
1.4 Future View 1
1.5 Cybercrime 2
1.5.1 SWOT Analysis 2
1.5.2 Current Threats 2
1.5.3 Current Defenses 2
1.5.4 Future Threats 2
1.5.5 Future Defenses 2
1.6 Cyberterrorism 2
1.6.1 SWOT Analysis 2
1.6.2 Current Threats 2
1.6.3 Current Defenses 3
1.6.4 Future Threats 3
1.6.5 Future Defenses 3
1.7 Gap Analysis 3

Figure 1 – Document Structure

Due to this proposal, all views will have the same structure, allowing alignment between the views and the different scenarios, especially considering gap analysis, as well as the development of a comprehensive roadmap:

- **Driving Forces**: This contains a list of social factors that are the driving forces like the contextual environment, society or other.

- **Current View**: Description of the current situation with respect to social and cultural characteristics.
- **Future View**: Analysis of recent developments that lead to future changes and to a situation that is different from the current one.
- **SWOT-Analysis**: Diagram on the strengths, weaknesses, opportunities and threats – for the cyber criminals as well as cyber terrorist's point of view.
- **Current Threats**: Current cybercrime-related threats that can be applied to the view.
- **Current Defenses**: Current defenses for protection against cybercrime for this view.
- **Future Threats**: Possible future cybercrimes relating to this view.
- **Future Defenses**: Analysis what techniques are needed in order to protect against future threats, as well as current threats where there currently is no countermeasure available.
- **Gap Analysis**: A structured approach targeting the research gaps – what can be applied to what view, what is missing and needs to be researched?

3.3 COORDINATION WITH CAMINO AND COURAGE

The coordination between the three projects CAMINO, COURAGE and CyberRoad was requested by the European Commission after the mid-project reviews. This is especially interesting and challenging, since the approaches towards roadmap construction have been developed independently by all three projects and thus the alignment must be done in a very structured way. Still, the final roadmap may benefit drastically from the cooperation between three different approaches in terms of completeness and expertise involved. In order to set up a structured approach towards this task, the three projects provided a written proposal, detailing how to achieve that in the past.

At the Workshop in Vienna it was mainly discussed, how to set up the CyberRoad-parts in order to integrate with the results from the other projects, as well as on the topic of refocusing certain tasks in order to better interface with the other project approaches. Since due to different approaches the status of the actual project-specific final roadmaps are at different stages, all projects go for the development of a set of preliminary results for a joint event taking place in The Hague on March 10 to March 11. During the Vienna meeting, several issues regarding the development of preliminary results using our methodology were discussed and solved accordingly.

3.4 OVERALL CONCLUSION

Taking into account the results and the feedback gathered, the second ARES-Workshop was a great success, especially considering the following developments that are vital for the further finalization of the project research roadmap:

- Generation and delimitation of the fundamental scenarios.
- Selection and delimitation of the views.
- Defining a strategy for alignment with the projects CAMINO and COURAGE, especially considering the topic of the generation of a unified roadmap containing an unambiguous and comprehensive gap analysis and the results of all three projects.

- Wrapping up the results from the First International Workshop on Future Scenarios for CyberCrime and CyberTerrorism (FCCT) and lessons learned with respect to future installments of FCCT.
- A project roadmap concerning the further project development based on the current status for the next 5 months.

4.1 WORSHOP ORGANIZATION

The Workshop was held on Thursday 10th and Friday 11th in the "International Press Centre Nieuwspoort" in the Hague, The Netherlands.

Agenda:

Thursday 10th:

- 13:30 – 14:00: Registration
- 14:00 – 14:05: **Welcome/introduction** – Gabriela Bodea, TNO
- 14:05 – 14:45: **Keynote** speech: "Cyber Terrorism: wrong assumptions & true facts: what I hope will never happen" – Raoul Chiesa, Security Brokers Italy
- 14:45 – 16:15: **Session 1**: Law and Law Enforcement (needs, challenges, solutions and practice) – Moderator: Cormac Callanan (Aconite)
- 16:15 – 16:30: Coffee break
- 16:30 – 18:00: **Session 2**: Solutions for the future: COURAGE-CAMINO-CyberROAD ideas
    - Working Session with audience
- 18:00 – 19:00: Networking Reception

Friday 11th:

- 09:30 – 10:45: **Session 3**: Citizens, Enterprise and Private Industry (needs, challenges, solutions and practice) – Moderator: Davide Ariu (University of Cagliari)
- 10:45 – 11:15: Coffee Break
- 11:15 – 12:45: **Session 4**: Government, Policy, Strategies and Awareness Raising - Moderator: Luigi Rebuffi (EOS)
- 12:45 – 13:45: Lunch
- 13:45 – 14:55: **Session 5**: Emerging Technologies and Solutions (including legal considerations, best practices etc.) - Moderator: Michal Choras (ITTI)
- 14:55 – 15:05: Coffee Break
- 15:05 – 16:00: **Wrap-up** and final Q&A

4.2 WORKSHOP PARTICIPANTS

Camino:

- Michal Choras

Courage:

- Babak Akhgar

CyberRoad:

- Davide Ariu

5.1 *WORKSHOP TARGET*

The target of the Workshop in The Hague was to develop a single Roadmap from the three different approaches at roadmap building that were devised by the three sister projects Courage, Camino and CyberRoad. The work on this Workshop can be seen as a consolidation response to the first joint Workshop between the three projects held in Brussels on June 4th 2015.

5.2 *THE THREE APPROACHES*

All three projects worked along different approaches in order to get a better understanding on all facettes of the given problem at hand – detecting the most important and relevant issues regarding cybercrime and cyber terrorism in context of actual or freseable new developments, together with the subsequent development iof a research roadmap for enabling better understanding of the dangers and possible mitigation strategies. The strategy of using different approaches for the same problem reduces the problem of implicit pre-selection of topics implied by the generation process of the roadmap itself, thus allowing a more complete view on the subject matter.

In case of cybercrime and cyberterrorism, the involvement of different partners with different agendas and often different base definitions, based on the different national jurisdictions by the member states, added another angle to the problem analysis.

- The development of the ***Camino***-Roadmap is primarily based on the THOR-approach, analysing new threats an countermeasures according to technical, human, organisational and regulatory dimensions.
- The ***Courage*** approach is based on three pillars: (I) A user centric methodology based on consultation of stakeholders and experts, (II) the generation of a taxonomy and common understanding and (III) a tool-related dimension to foster practical implementations of countermeasures using effective test and validation solutions.
- ***CyberRoad*** uses explorative scenario building, where experts and stakeholders identified lasting and new trends in the development of our modern digital society. Future development of and threats to these trends were extrapolated and the current state of countermeasures evaluated. The resulting gaps form the basis for the proposed roadmap.

5.3 *THE THOR-APPROACH*

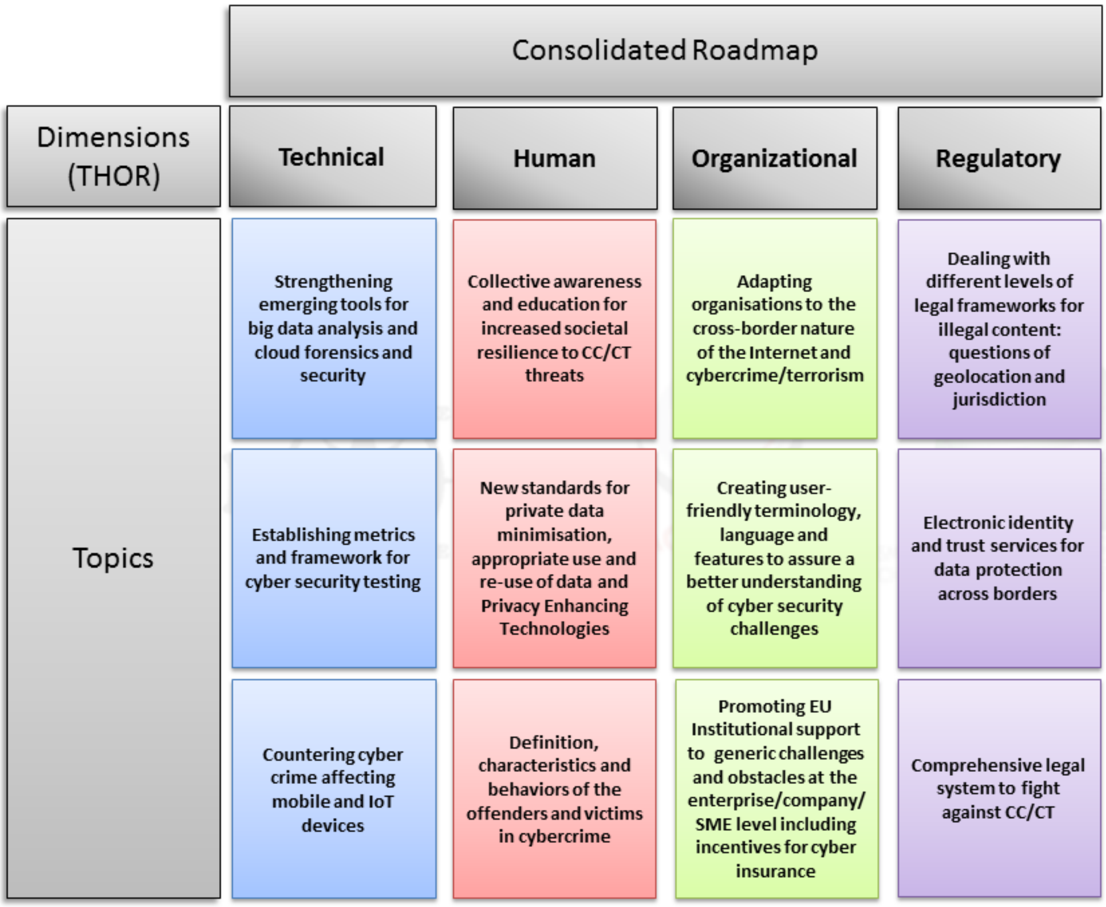
On the meeting it was decided to structure the results from the three roadmpas along the THOR-dimensions:

- The ***Technical*** dimension covers all technological aspects that can be ised for fighting acts of cybercrime and cyberterrorism.
- The ***Human*** dimension is related to behavioural aspects and “soft” issues like raising awareness, but also to dangers to personal privacy and treatment of sensitive data.

- The ***Organisational*** dimension covers topics on the organisational level, especially considering policies and cooperations between organisations, also between entities from different backgrounds like public entities (e.g. LEAs) cooperating with private institutions or companies.
- The ***Regulatory*** dimension covers topics related to the legal aspects of fighting cybercrime and cyberterrorism like legal changes and standardisation.

5.4 *THE CONSOLIDATED ROADMAP*

For every dimension, three topics were identified to be of the highest importance for a future research roadmap and were thus identified to be the cornerstones of the consolidated research roadmap of al three projects.



	Consolidated Roadmap			
Dimensions (THOR)	**Technical**	**Human**	**Organizational**	**Regulatory**
Topics	Strengthening emerging tools for big data analysis and cloud forensics and security	Collective awareness and education for increased societal resilience to CC/CT threats	Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism	Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction
	Establishing metrics and framework for cyber security testing	New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies	Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges	Electronic identity and trust services for data protection across borders
	Countering cyber crime affecting mobile and IoT devices	Definition, characteristics and behaviors of the offenders and victims in cybercrime	Promoting EU Institutional support to generic challenges and obstacles at the enterprise/company/ SME level including incentives for cyber insurance	Comprehensive legal system to fight against CC/CT

Figure 2 – Overview over the core topics

5.5 *THE TECHNICAL DIMENSION*

The following three topics were identified as most central for a research roadmap on cybercrime and cyberterrorism with respect to the technical dimension:

- ***Strengthening emerging tools for big data analysis and cloud forensics and security***: This topic is especially focusing on the utilization of big data technologies in order to enable better detection of attacks through pattern matching and correlation of data, also data derived from different sources.

- ***Establishing metrics and framework for cyber security testing:*** This topic mainly focusses on issues related to making security measurable, which is needed for building test beds. Also, this topic includes the development of open test beds for testing cyber security, sharing information about vulnerabilities and other issues, especially related to the "security by design" principle.
- ***Countering cyber crime affecting mobile and IoT devices****:* The main issues in this topic are related to the increasing spread of mobile malware, not only related to classical smartphones, but also to the upcoming IoT-domain. This includes means for detecting bot nets, as well as the development of robust countermeasures.

5.6 THE HUMAN DIMENSION

The following three topics were identified as most central for a research roadmap on cybercrime and cyberterrorism with respect to the human dimension:

- ***Collective awareness and education for increased societal resilience to CC/CT threats***: The main focus of this topic lies in the development of new strategies for raising awareness and educating stakeholders across all levels of society. This also includes new and emerging technologies and their subsequent misuse as attack vectors.
- ***New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies***: The roadmap will mainly be concerned with issues of data privacy and the subsequent use of data that was originally collected for other purposes by LEAs and the resulting legal issues. This also includes technologies for minimizing the use of private data.
- ***Definition, characteristics and behaviors of the offenders and victims in cybercrime****:* In order to allow efficient battling of cybercrime and cyberterrorism, it is important to understand the different actors involved, on the attacker, as well as on the victim side.

5.7 THE ORGANISATIONAL DIMENSION

The following three topics were identified as most central for a research roadmap on cybercrime and cyberterrorism with respect to the organisational dimension:

- ***Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism***: One of the main obstacles in international cooperation for fighting cybercrime and cyberterrorism lies in the different laws and regulatory issues, especially considering laws against sharing of vital information. Homogenisation of laws and enabling the cooperation between CERTs and LEAs of different member states is on of the main cornerstones of the roadmap.
- ***Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges***: Harmonising terminology is one of the most important baseline issues that needs to be solved in order to allow for effective combating of cybercrime and cyberterrorism, as well as for enhancing research on these topics. This needs

to lead to a set of standardized terms and definitions that are understood in the same way throughout Europe.

- ***Promoting EU Institutional support to generic challenges and obstacles at the enterprise/company/SME level including incentives for cyber insurance***: It is of the utmost importance that critical developments in fighting cybercrime and cyberterrorism are brought to the companies and accepted by the industry as important. Thus, common support is needed on a European level.

5.8 THE REGULATORY DIMENSION

The following three topics were identified as most central for a research roadmap on cybercrime and cyberterrorism with respect to the regulatory dimension:

- ***Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction:*** The main focus of this topic lies in the development of methods that allow LEAs better gathering and sharing of relevant information across national borders, as well as developing standards for collaboration between the governmental and the private sectors.
- ***Electronic identity and trust services for data protection across borders:*** This cornerstone covers direly needed research work in the areas of authentication & signature regulations, as well as e-identity.
- ***Comprehensive legal system to fight against CC/CT:*** The legal systems need to be improved in order to facilitate transparent and comprehensive treatments of all phases of a cybercrime case, especially including the improvement of forensic procedures, as well as insuring the best possible information flow between the separate stages of an investigation.

6.1 CYBERROAD INTERNAL MEETING IN VIENNA – AGENDA

****

CyberROAD Meeting - December 9, 2015 - Vienna
AGENDA

- **10.30 - 11.00** - Welcome
- **11 A.M. - 11.30 A.M.**
  - **Session Leader: Davide Ariu**
    - Topics:
      - General Update on the Project
      - Coordination Among T3.3, T5.4, and T6.4 for the preparation of the Scenarios
      - After the Scenarios: final steps toward the CyberROAD roadmap
      - Update on WP3 Scenarios
- **11.30 A.M. - 12.15 A.M.**
  - **Session Leader: Piotr Kijewski**
    - Update on the WP5 Scenarios and Discussion
      - List of the scenarios proposed
      - Motivations for each scenario
      - Key contents of the scenario
      - Sources of information for each scenario
      - How is the work for the development of each scenario being organised (partners involved).
- **12.15 A.M. - 1.00 P.M.**
  - **Session Leader: Elisa Costante**
    - Update on the WP6 Scenarios and Discussion
      - List of the scenarios proposed
        - Motivations for each scenario
        - Key contents of the scenario
        - Sources of information for each scenario
        - How is the work for the development of each scenario being organised (partners involved).
- **1 P.M. - 2.15 P.M. - Lunch Break**
- **2.15 P.M. - 3 P.M.**
  - **Session Leader: Olga Segou**
    - Update on the WP7 Activities and Plan for the last months
- **3 P.M. - 3.30 P.M.**
  Any Other Business

****

6.2 CYBERROAD INTERNAL MEETING IN VIENNA – WP5-WP6 SLIDES

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

WP3/WP5/WP6

Cyber Crime/Terrorism Research Topics

Scenarios Selection and Plan

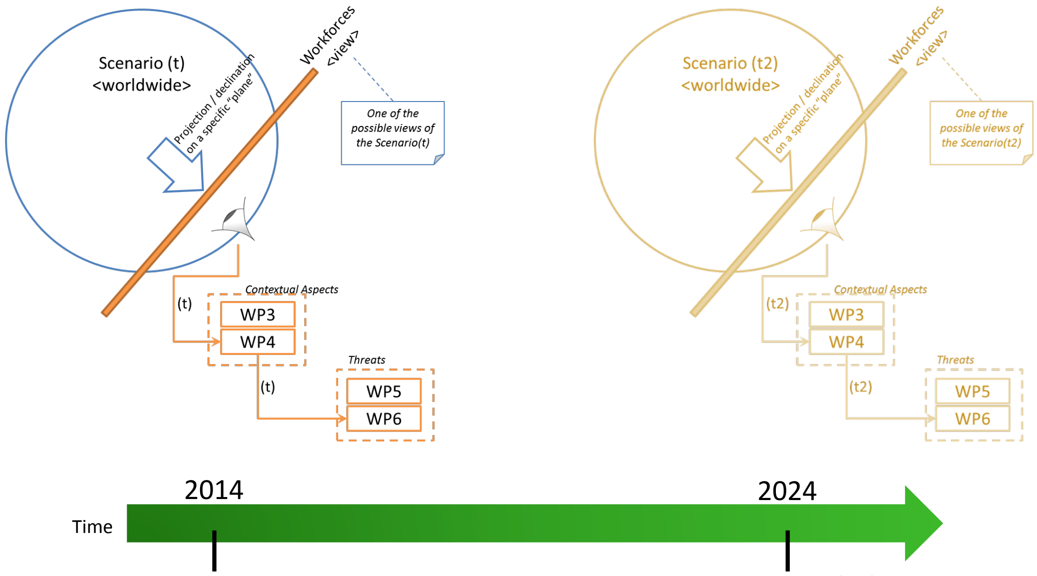
VIENNA 09/12/2015

Elisa Costante- SecurityMatters- elisa.costante@secmatters.com
Piotr Kijewski – NASK – piotr.kijewski@cert.pl

SECURITY MATTERS *Rethink Cybersecurity*

CERT.PL >_

Scenario vs Views


Scenario (t)
<worldwide>
Projection / declination on a specific "plane"
Workforces <view>
One of the possible views of the Scenario(t)
Contextual Aspects
(t)
WP3
WP4
Threats
(t)
WP5
WP6
Scenario (t2)
<worldwide>
Projection / declination on a specific "plane"
Workforces <view>
One of the possible views of the Scenario(t2)
Contextual Aspects
(t2)
WP3
WP4
Threats
(t2)
WP5
WP6
2014
2024
Time

Scenario (t)
The current state

Scenario (t2)
The future state

Scenario vs View

- A scenario includes multiple views
  - Example:
    - **Scenario**: Social Sharing
    - **Views**: Social Networks, Life logging, Wearable devices
- **Partners** will be assigned to views
  - A view should be described by filling a predefined template
- The **WP leaders** will take care of
  - describing the scenarios
  - merging the contributions
  - avoid overlaps

Selected Scenarios and Views

Scenario	View	Partner
Social Sharing	(i) Social Network (CC and CT)	NASK & FORTH
	(ii) Life logging (CC and CT)	RHUL
	(iii)Wearable device (CC & CT)	SUPSI
Building Automation	(i) Smart Building and domotics	SBA
Energy	(i) Water Utilities	SM
	(ii) Gas Utilities	VITRO
	(iii) Smart Grid	VITRO
Transportation	(i) ICT Systems for Transportation	NCSRDD
	(ii) Aviation	NCSRDD
	(iii) Smart Roads	NCSRDD
Healthcare	(i) Mobile Health and Augmented Humans	CEFRIEL
	(ii) Hospital 2.0	CEFRIEL
	(iii) P4 Medicine	SBA
Security and safety	(i) Fighting Cybercrime as a Service	CDF
	(ii) Attribution of cyber crime	NASK
	(iii) Trusted Components (SW and HW, supply chain)	TUD
Workforce	(i) Enterprise 2.0 (BYOD, ubiquitous connectivity)	CEFRIEL
Industry	(i) Industry 4.0	SM
	(ii) Just in time production	TUD
Financial Services	(i) Cryptocurrencies	CDF
	(ii) Online Banking	RHUL
Data Driven Economy	(i) Big Data (CC and CT)	SBA
	(ii) Control over data (includes privacy, data protection and leakage, OS/computer system logging, Software as a Service (SaS))	SBA

View Document Structure

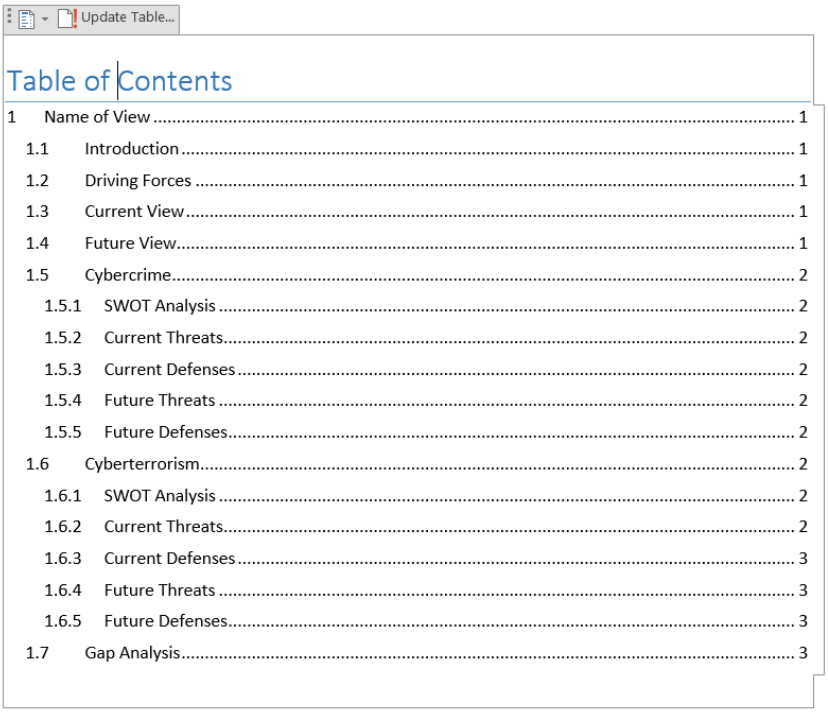


Table of Contents

1 Name of View 1
1.1 Introduction 1
1.2 Driving Forces 1
1.3 Current View 1
1.4 Future View 1
1.5 Cybercrime 2
1.5.1 SWOT Analysis 2
1.5.2 Current Threats 2
1.5.3 Current Defenses 2
1.5.4 Future Threats 2
1.5.5 Future Defenses 2
1.6 Cyberterrorism 2
1.6.1 SWOT Analysis 2
1.6.2 Current Threats 2
1.6.3 Current Defenses 3
1.6.4 Future Threats 3
1.6.5 Future Defenses 3
1.7 Gap Analysis 3

Plan of Actions

- Current work directory: **CyberROAD \WP2\Scenarios_D3.3-D5.6-D6.6\views(current-work-directory)** contains:
  1. **Assignment.pptx** (this presentation)
  2. **Template-and-instructions.docx** contains instructions on what contents are expected in what section
  3. **Example-Social-Network-View.docx** contains a **complete example** for the social network view.

- Contributions
  1. For **every view** the partner should fill in the template
     - partners that have already provided contributions are asked to adapt it to the new template and add the missing parts
  2. For **every view**, the partner should analyze both the cybercrime (CC) and the cyber terrorism (CT) perspective
  3. Deadline is **January 4th 2016**

6.3 CYBERROAD INTERNAL MEETING IN VIENNA – WP7 SLIDES

CYBER ROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

European Commission
Seventh Framework Programme

Update on the Project Activities

WP7 Dissemination and Exploitation

Olga E. Segou, PhD
Stelios C.A. Thomopoulos, PhD
National Centre for Scientific Research "Demokritos"
Institute of Informatics and Telecommunications
Integrated Systems Laboratory

CyberROAD Project Meeting – December 9th , 2015

WP7 – Current State

- **Leader:** NCSRD
- **Participants:** All
- **Start:** M1 **End:** M24

- **WP7 Objectives for Year 2**
  - Dissemination and Exploitation actions
  - **Liaison Database**
  - Setting up the Final Event
  - **Awareness training**
  - **Video production**

- **Tasks:**
  - T7.1 – Planning – NCSRD
  - T7.2 – Liaison Database – NCSRD
  - T7.3 – Establishment of a digital presense – FORTH
  - T7.4 – Workshops and Publications – SBA
  - T7.5 – Generalized Awareness and Training Campaign – UNICA
  - T7.6 – Final Event – UNICA

Deliverable 7.4 - Liaison Database

- **Task:** T7.2 **Delivery Date:** M24
- **Status:** In Progress **Actual Del. Date:** internal delivery by M20
- **Leader:** NCSRD
- **Partners:** CEFRIEL, SUPSI

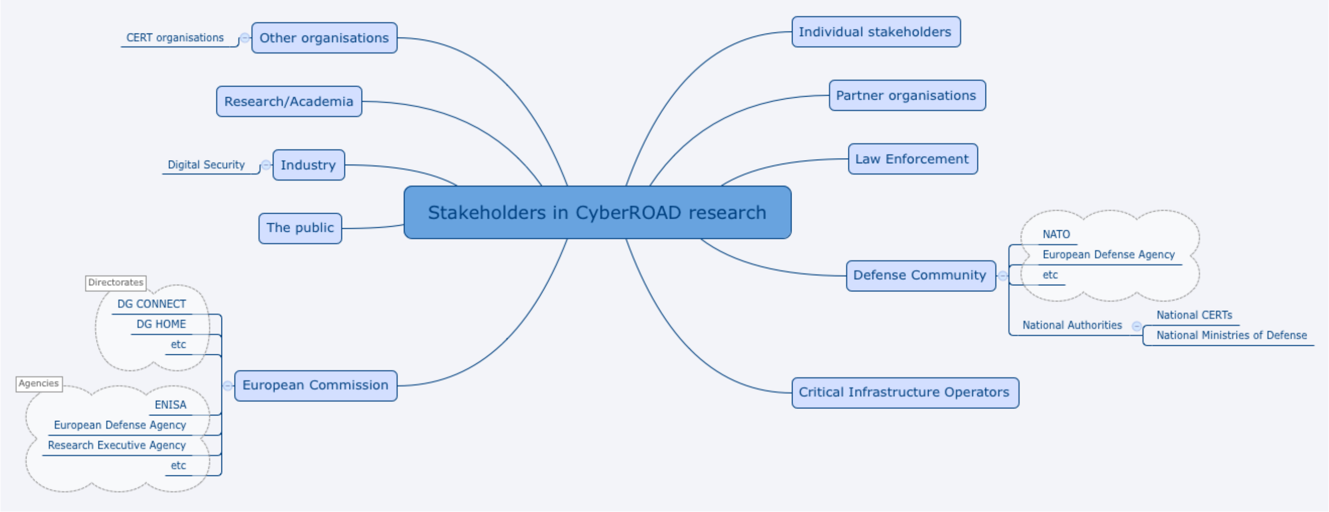
- **Task summary**
  - Contact database for dissemination and exploitation
  - Utilized to send invitations to the final event
  - **Stakeholder mapping for Cyber Crime and Cyber Terrorism research**
  - Relevant contents/outcomes toward the preparation of the roadmap

- **Issues emerged during the preparation of the deliverable**
  - Forms etc. are available in Own Cloud
  - Partners don't generally use the reporting forms for WP7 (Liaison Database included)
  - We need to jumpstart the task and have a draft ready before we start preparations for the project's final event

Deliverable 7.4
Liaison Database

- **Way forward: Stakeholder analysis**
  - Define an **appropriate methodology & visualisation** type
  - **List** stakeholder types and stakeholders
  - Provide KPIs to measure **stakeholder impact**
  - Assess **their importance and influence**
  - Define **our expectations from each stakeholder** (what kind of contribution are we expecting, what level of involvement)
  - Provide **a liaison plan** for each stakeholder type & execute the plan (i.e. contact, invite to final event, send dissemination material etc)

D7.4 Mindmap Example



Stakeholders in CyberROAD research

Other organisations

CERT organisations

Research/Academia

Industry

Digital Security

The public

European Commission

Directorates

DG CONNECT

DG HOME

etc

Agencies

ENISA

European Defense Agency

Research Executive Agency

etc

Individual stakeholders

Partner organisations

Law Enforcement

Defense Community

NATO

European Defense Agency

etc

National Authorities

National CERTs

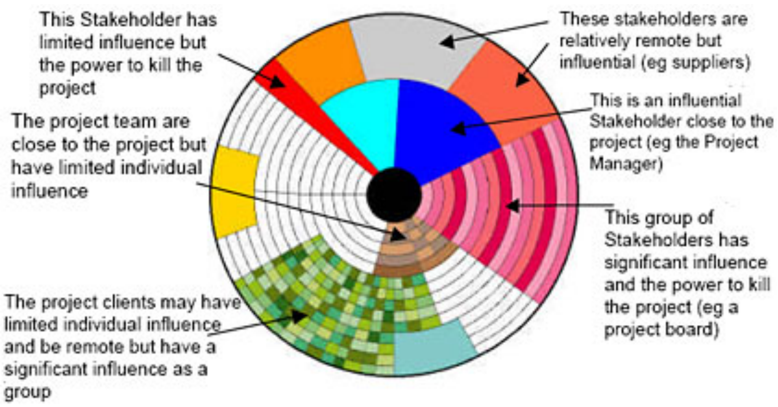
National Ministries of Defense

Critical Infrastructure Operators

Fig 1: Brainstorming on stakeholder types

D7.4 Stakeholder mapping

Examples:



This Stakeholder has limited influence but the power to kill the project

The project team are close to the project but have limited individual influence

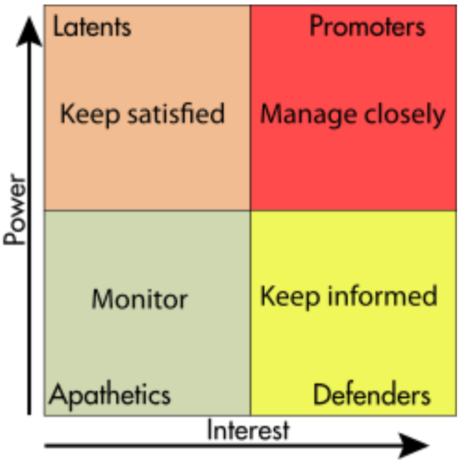
The project clients may have limited individual influence and be remote but have a significant influence as a group

These stakeholders are relatively remote but influential (eg suppliers)

This is an influential Stakeholder close to the project (eg the Project Manager)

This group of Stakeholders has significant influence and the power to kill the project (eg a project board)

Fig 2: Stakeholder Circle (trademarked concept)



Latents

Keep satisfied

Promoters

Manage closely

Monitor

Apathetics

Keep informed

Defenders

Power

Interest

Fig 3: Stakeholder Matrix
(Power v Interest, Influence v Interest, 3D Influence v attitude v interest etc.)

Dissemination video

- **Script a dissemination video for CyberROAD**
  - Mostly use of animation
  - Ideally a 3 min video would suit the project (Minimum duration 2 minutes, maximum 5 minutes)
  - Production time varies depending on the content

  What needs to be done:
  - Discuss the script elements
  - Focus on WP achievements and methodology and avoid project “jargon”
  - Will be discussed with project Coordinator and WP leaders

  Necessary elements:
  - Introduction to the project,
  - Introduction of consortium
  - Acknowledgement to the European Commission
  - **Why is Cyber Road important (metrics?)**
  - **What we do**

D7.5 Awareness campaign

- **Task 7.5** is dedicated to public awareness
  - Training activities within partners
  - Reaching out to the general public
- **Leader:** UNICA
- **Partners:** INDRA, POSTEIT, VITROCISET, INOV, NCSRD, NASK, PJ, CYBERDEFCON, HMOD, MCAFEE, MELANI
- **What are the training activities that we can schedule within our organisations?**
- **Disseminate material (through our public relations departments) targeted to the public**
  - Examples:
    - Students/Pupils: Social media, privacy, e-bullying, etc
    - SMEs: Cyber Security essentials
    - Parents: parental controls for safe internet
    - Others?
- **Decide the kind of dissemination material to design and the content**

Thank you for your attention

6.4 CYBERROAD-CAMINO-COURAGE WORKSHOP IN THE HAGUE – AGENDA

FINAL AGENDA:

COURAGE – CAMINO – CyberROAD joint conference on "Emerging and Current Challenges in Cybercrime and Cyberterrorism"

Thursday 10 and Friday 11 March 2016

International Press Centre Nieuwspoort in The Hague, Netherlands

<table>
<tr><th colspan="2">Thursday 10 March 2016</th></tr>
<tr><td>13:30-14:00</td><td><i>Registration and Coffee</i></td></tr>
<tr><td>14:00-14:05</td><td>Welcome/introduction – <b>Gabriela Bodea, TNO</b></td></tr>
<tr><td>14:05-14:45</td><td>Keynote speech – <b>Raoul Chiesa, Security Brokers Italy</b>
"Cyber Terrorism: wrong assumptions & true facts: what I hope will never happen"</td></tr>
<tr><td>14:45-16:15</td><td>Session 1: Law and Law Enforcement (needs, challenges, solutions and practice)
Moderator: <b>Cormac Callanan (Aconite)</b>
<table>
<tr><td>14:45 – 15:05</td><td>DI. Geoff Halpin</td><td>Yorkshire and Humberside Regional Cybercrime Unit</td></tr>
<tr><td>15:05 - 15:25</td><td>Pim Takkenberg</td><td>TNO</td></tr>
<tr><td>15:25 - 15:45</td><td>Jerzy Kosinski</td><td>WSPol Szczytno – Higher School of the Police</td></tr>
<tr><td>15:45-16:05</td><td>Judyta Kasperkiewicz</td><td>University of Silesia in Katowice, Faculty of Law and Administration, Department of Forensic Science</td></tr>
<tr><td>16:05 - 16:15</td><td colspan="2"><i>Q&amp;A</i></td></tr>
</table></td></tr>
<tr><td>16:15-16:30</td><td><i>Coffee break</i></td></tr>
<tr><td>16:30-18:00</td><td>Session 2: Solutions for the future: COURAGE-CAMINO-CyberROAD ideas
<b>Babak Akhgar</b>, representative of the European project COURAGE
<b>Michal Choras</b>, representative of the European project CAMINO
<b>Davide Ariu</b>, representative of the European project CyberROAD</td></tr>
</table>

The COURAGE project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949

	Working session with audience
18:00-19:00	*Networking reception*

<table>
<tr><th colspan="2">Friday 11 March 2016</th></tr>
<tr><td>9:30-10:45</td><td>Session 3: Citizens, Enterprise and Private Industry (needs, challenges, solutions and practice)
Moderator: <b>Davide Ariu (University of Cagliari)</b>
<table>
<tr><td>9:30 - 9:50</td><td>Gary Hibberd</td><td>Agenci UK</td></tr>
<tr><td>9:50 - 10:10</td><td>Rocco Mammoliti / Massimiliano Aschi</td><td>Poste Italiane</td></tr>
<tr><td>10:10 - 10:30</td><td>Dimitris Kavallieros</td><td>KEMEA/UINFC2 Project</td></tr>
<tr><td>10:30 - 10:45</td><td colspan="2"><i>Q&A</i></td></tr>
</table></td></tr>
<tr><td>10:45-11:15</td><td><i>Coffee break</i></td></tr>
<tr><td>11:15-12:45</td><td>Session 4: Government, Policy, Strategies and Awareness Raising
Moderator: <b>Luigi Rebuffi (EOS)</b>
<table>
<tr><td>11:15 - 11:35</td><td>Quentin Revell</td><td>UK Home Office Centre for Applied Science and Technology</td></tr>
<tr><td>11:35 -11:55</td><td>Robin de Haas</td><td>The Hague Security Delta</td></tr>
<tr><td>11:55 - 12:15</td><td>Stuart Hyde</td><td>CCL Group Ltd UK</td></tr>
<tr><td>12:15 - 12:35</td><td>Olivier Burgersdijk</td><td>EC3/Europol</td></tr>
<tr><td>12:35 - 12:45</td><td colspan="2"><i>Q&A</i></td></tr>
</table></td></tr>
<tr><td>12:45-13:45</td><td><i>Lunch</i></td></tr>
<tr><td>13:45-14:55</td><td>Session 5: Emerging Technologies and Solutions (including legal considerations, best practices etc.)
Moderator: <b>Michal Choras (ITTI)</b>
<table>
<tr><td>13:45 - 14:05</td><td>Dr Argyro Karanasiou</td><td>Bournemouth University</td></tr>
<tr><td>14:05 -14:25</td><td>Prof. Dr. Bert-Jaap Koops</td><td>Professor of regulation and technology, Tilburg University</td></tr>
<tr><td>14:25 -14:45</td><td>Prof Wojciech Mazurczyk</td><td>Fern University and PW, Warsaw</td></tr>
<tr><td>14:45 - 14:55</td><td colspan="2"><i>Q&A</i></td></tr>
</table></td></tr>
<tr><td>14:55-15:05</td><td><i>Coffee break</i></td></tr>
<tr><td>15:05-16:00</td><td>Wrap-up and final Q&A</td></tr>
</table>

The COURAGE project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949

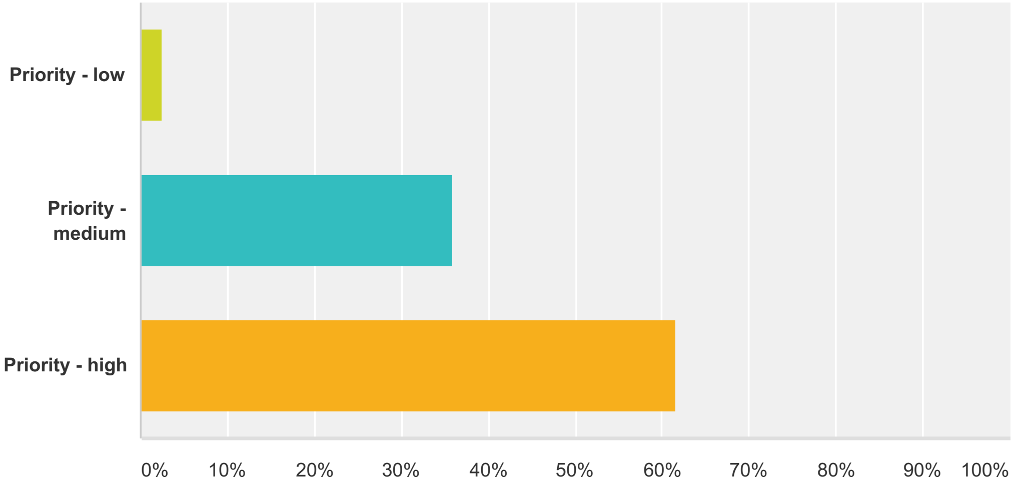
	Babak Akhgar, representative of the European project COURAGE **Michal Choras**, representative of the European project CAMINO **Davide Ariu**, representative of the European project CyberROAD

The COURAGE project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949

6.5 *CyberROAD-CAMINO-COURAGE Workshop in The Hague – Consolidated Roadmap Survey Results*

Q1 Strengthening emerging tools for big data analysis, cloud forensics and security

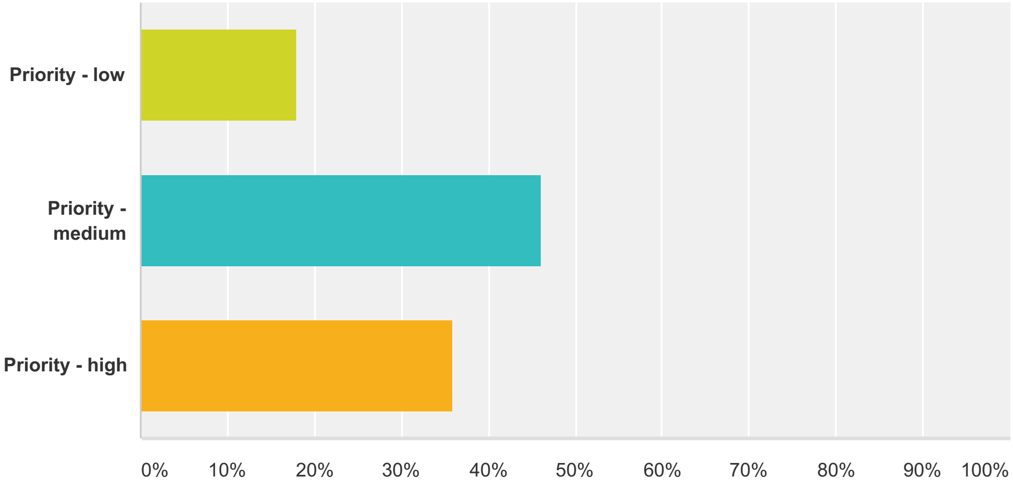
Answered: 39 Skipped: 0



Answer Choices	Responses	
Priority - low	**2.56%**	1
Priority - medium	**35.90%**	14
Priority - high	**61.54%**	24
Total		**39**

Q2 Establishing metrics and framework for cyber security testing

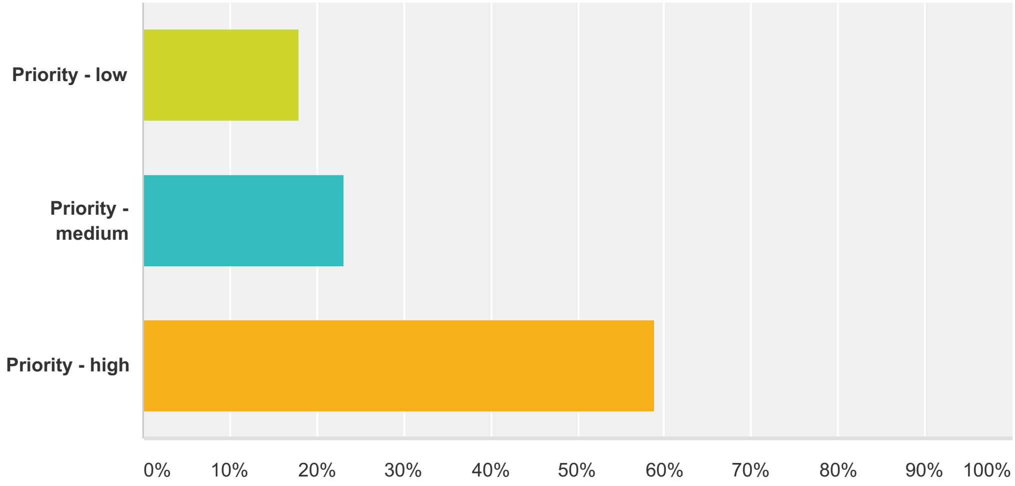
Answered: 39 Skipped: 0



Answer Choices	Responses	
Priority - low	17.95%	7
Priority - medium	46.15%	18
Priority - high	35.90%	14
Total		39

Q3 Countering cybercrime affecting mobile and IoT devices

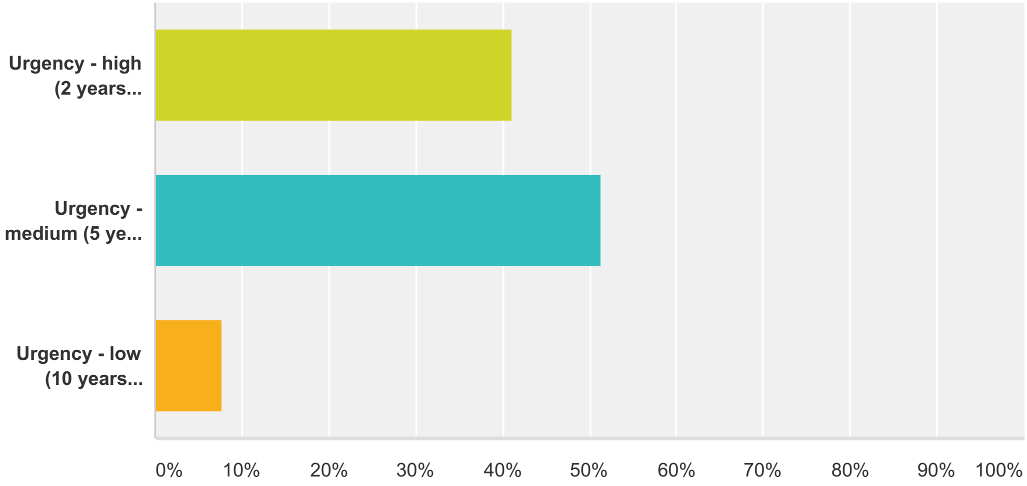
Answered: 39 Skipped: 0



Answer Choices	Responses	
Priority - low	**17.95%**	7
Priority - medium	**23.08%**	9
Priority - high	**58.97%**	23
Total		**39**

Q4 Strengthening emerging tools for big data analysis, cloud forensics and security

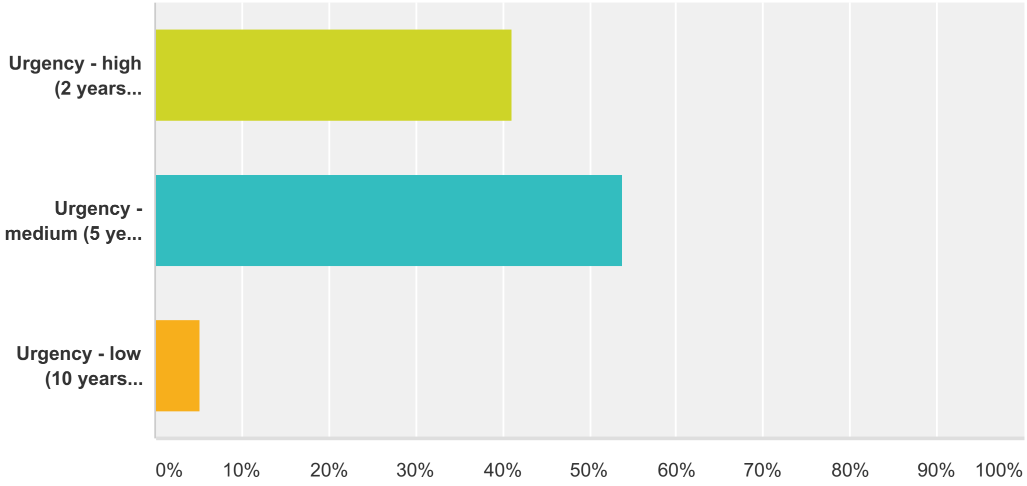
Answered: 39 Skipped: 0



Answer Choices	Responses	
Urgency - high (2 years perspective)	**41.03%**	16
Urgency - medium (5 years perspective)	**51.28%**	20
Urgency - low (10 years perspective)	**7.69%**	3
Total		**39**

Q5 Establishing metrics and framework for cyber security testing

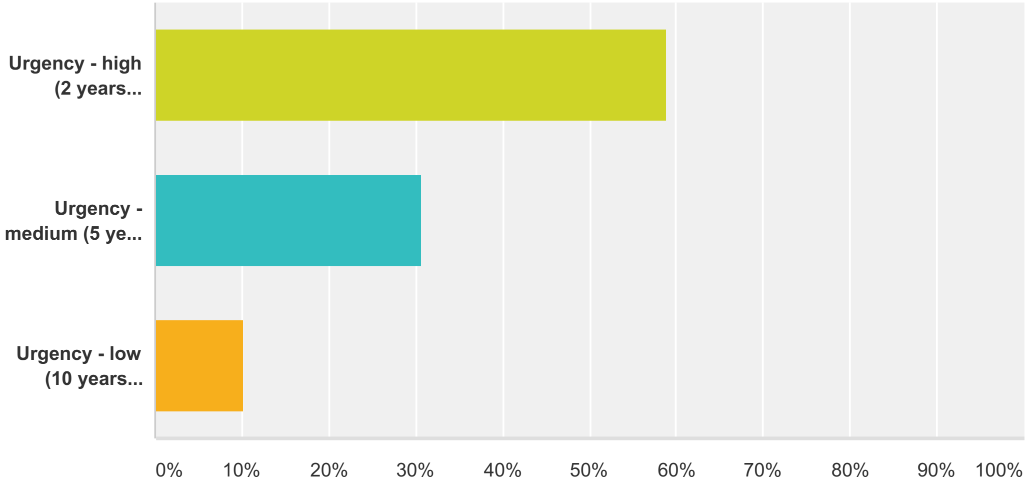
Answered: 39 Skipped: 0



Answer Choices	Responses	
Urgency - high (2 years perspective)	**41.03%**	16
Urgency - medium (5 years perspective)	**53.85%**	21
Urgency - low (10 years perspective)	**5.13%**	2
Total		**39**

Q6 Countering cybercrime affecting mobile and IoT devices

Answered: 39 Skipped: 0



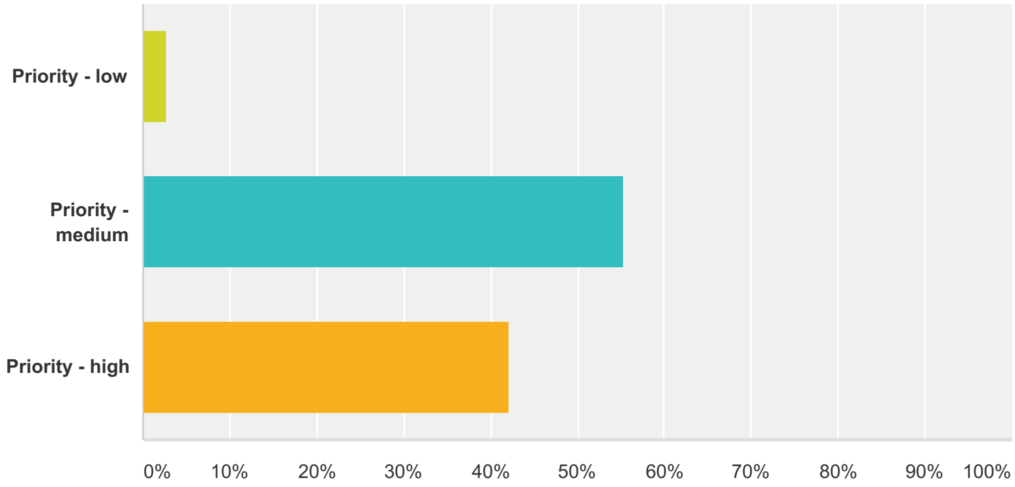
Answer Choices	Responses	
Urgency - high (2 years perspective)	**58.97%**	23
Urgency - medium (5 years perspective)	**30.77%**	12
Urgency - low (10 years perspective)	**10.26%**	4
Total		**39**

Q7 Additional Comments…

Answered: 3 Skipped: 36

Q8 Collective awareness and education for increased societal resilience to CC/CT threats

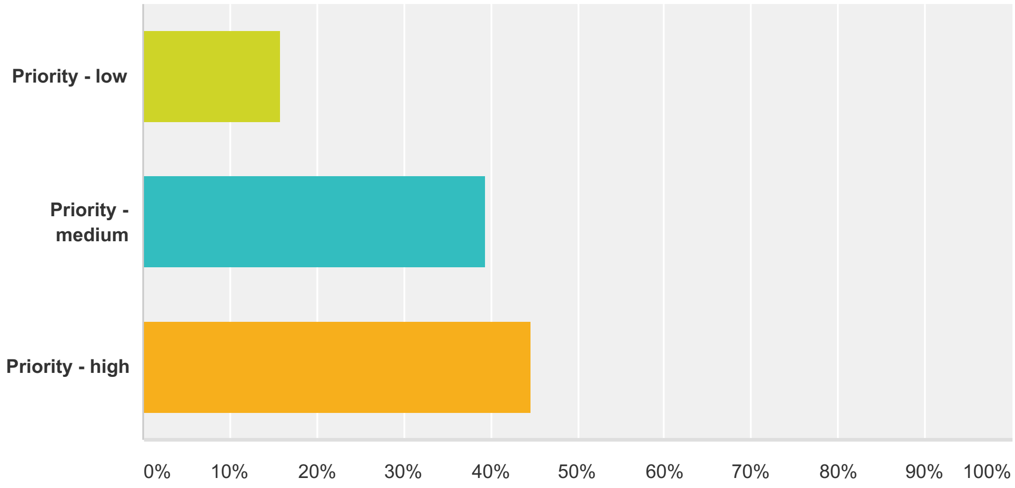
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	**2.63%**	1
Priority - medium	**55.26%**	21
Priority - high	**42.11%**	16
Total		**38**

Q9 New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies

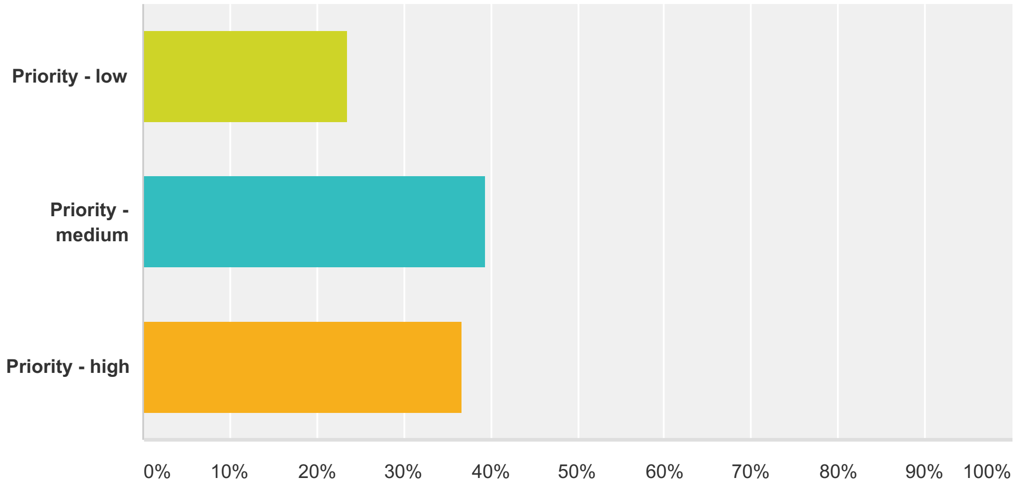
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	**15.79%**	6
Priority - medium	**39.47%**	15
Priority - high	**44.74%**	17
Total		**38**

Q10 Definition, characteristics and behaviours of the offenders and victims in cybercrime

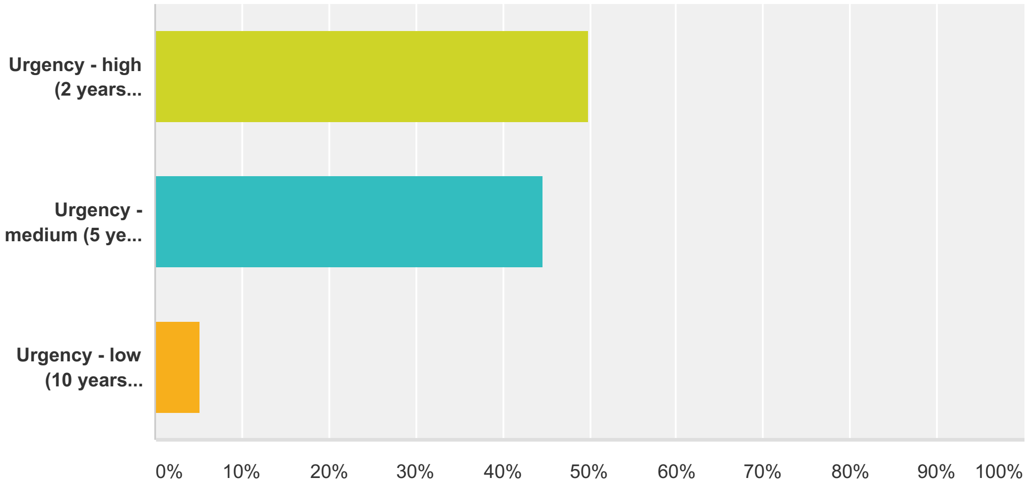
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	23.68%	9
Priority - medium	39.47%	15
Priority - high	36.84%	14
Total		38

Q11 Collective awareness and education for increased societal resilience to CC/CT threats

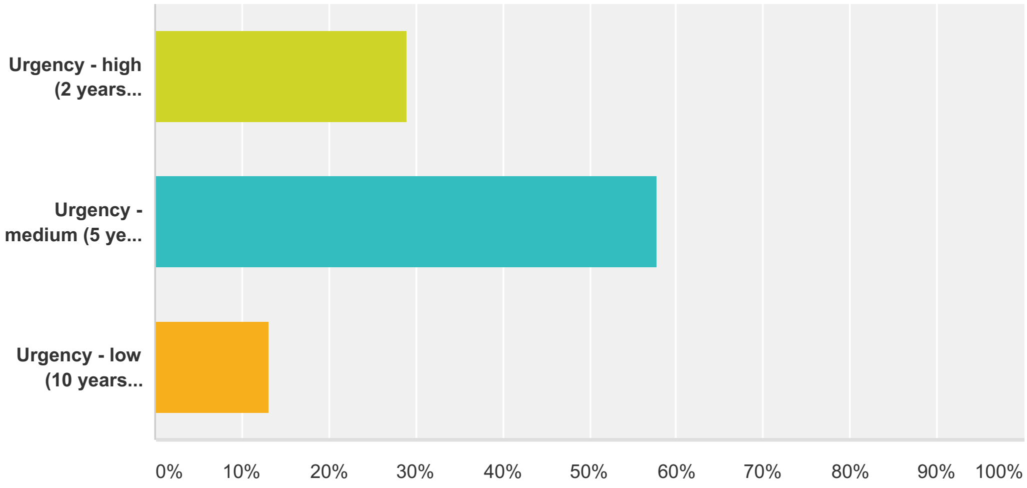
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**50.00%**	19
Urgency - medium (5 years perspective)	**44.74%**	17
Urgency - low (10 years perspective)	**5.26%**	2
Total		**38**

Q12 New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies

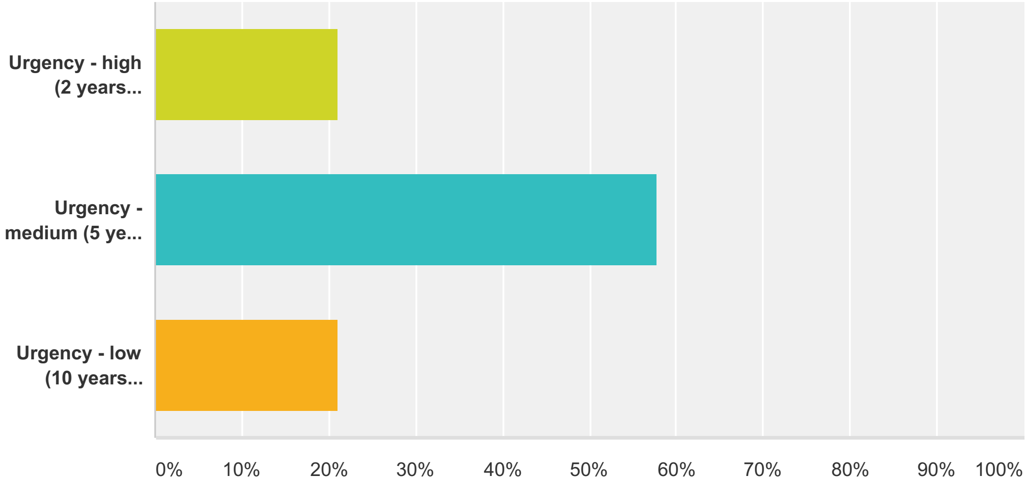
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**28.95%**	11
Urgency - medium (5 years perspective)	**57.89%**	22
Urgency - low (10 years perspective)	**13.16%**	5
Total		**38**

Q13 Definition, characteristics and behaviours of the offenders and victims in cybercrime

Answered: 38 Skipped: 1



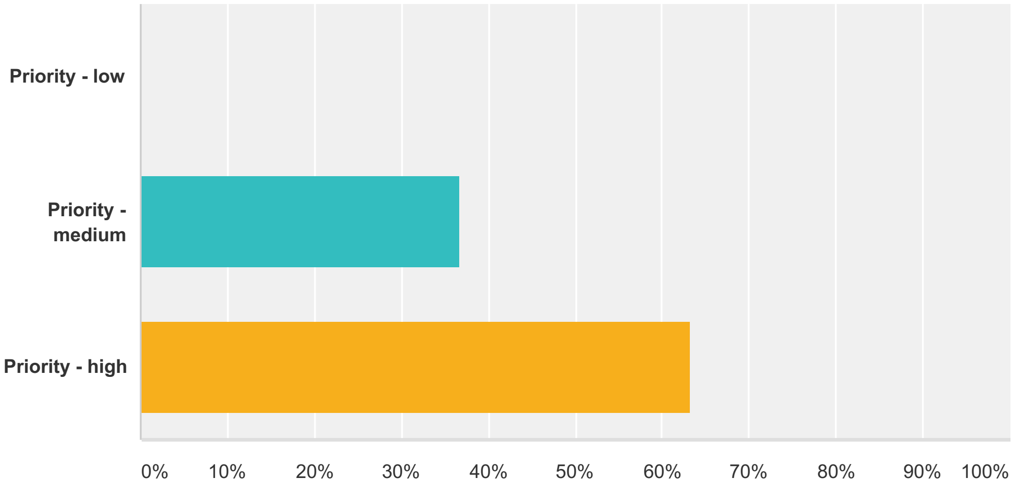
Answer Choices	Responses	
Urgency - high (2 years perspective)	**21.05%**	8
Urgency - medium (5 years perspective)	**57.89%**	22
Urgency - low (10 years perspective)	**21.05%**	8
Total		**38**

Q14 Additional Comments…

Answered: 0 Skipped: 39

Q15 Adapting organisations to the cross-border nature of the Internet and cybercrime/ terrorism

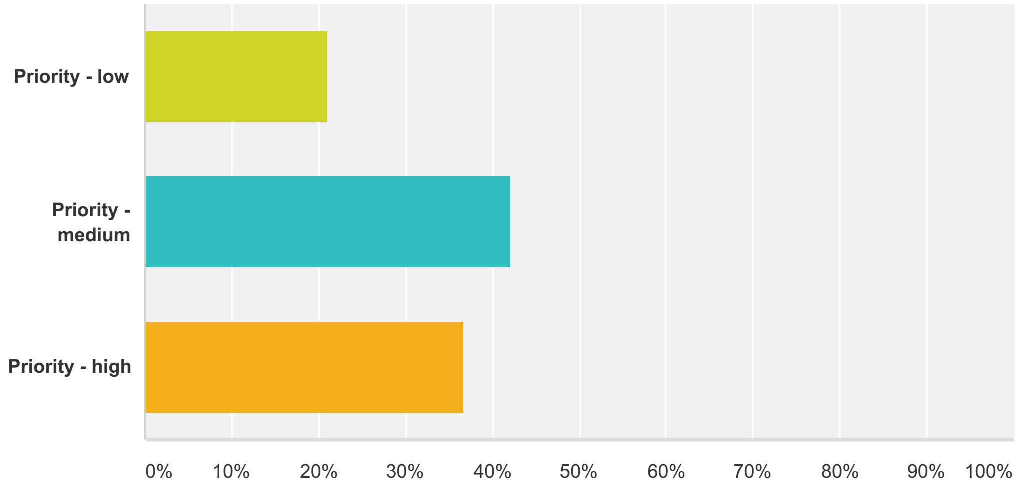
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	**0.00%**	0
Priority - medium	**36.84%**	14
Priority - high	**63.16%**	24
Total		**38**

Q16 Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges

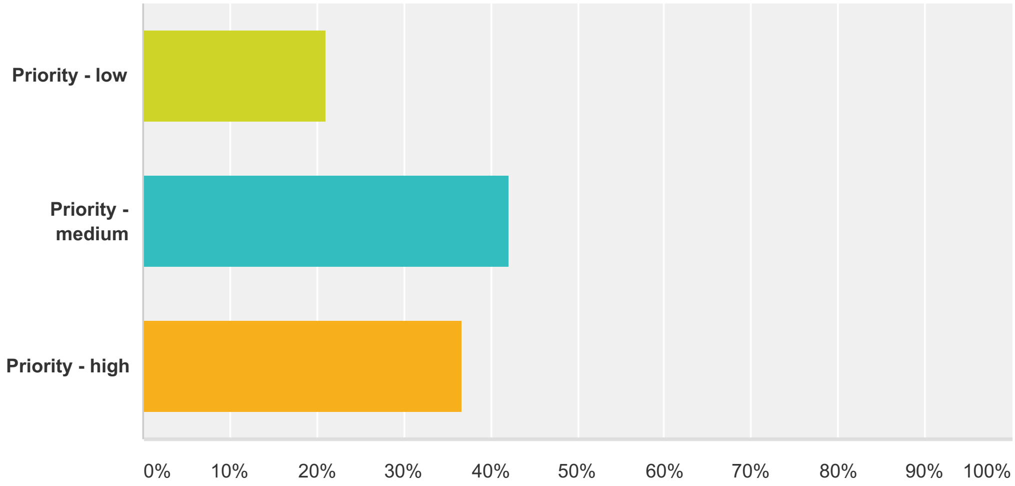
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	21.05%	8
Priority - medium	42.11%	16
Priority - high	36.84%	14
Total		38

Q17 Promoting EU Institutional support to generic challenges and obstacles at the enterprise/ company/ SME level including incentives for cyber insurance

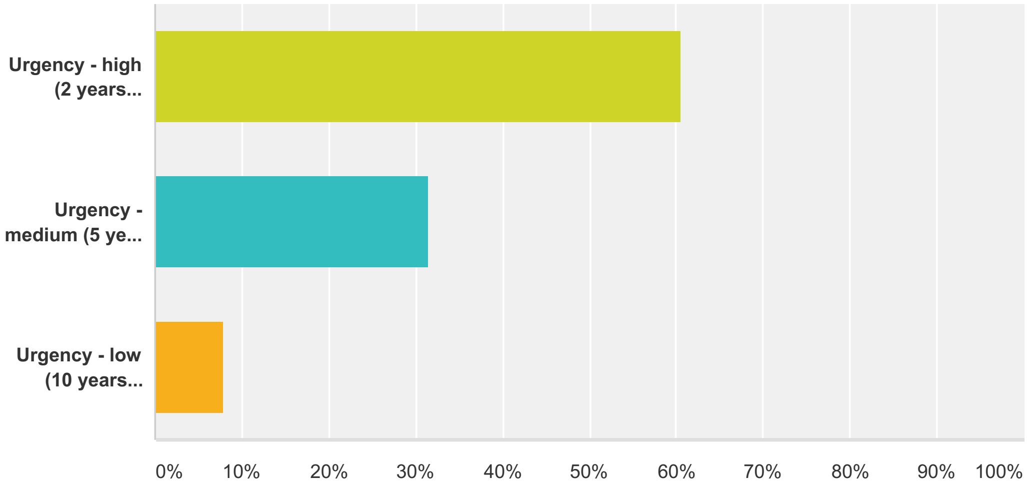
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	21.05%	8
Priority - medium	42.11%	16
Priority - high	36.84%	14
Total		38

Q18 Adapting organisations to the cross-border nature of the Internet and cybercrime/ terrorism

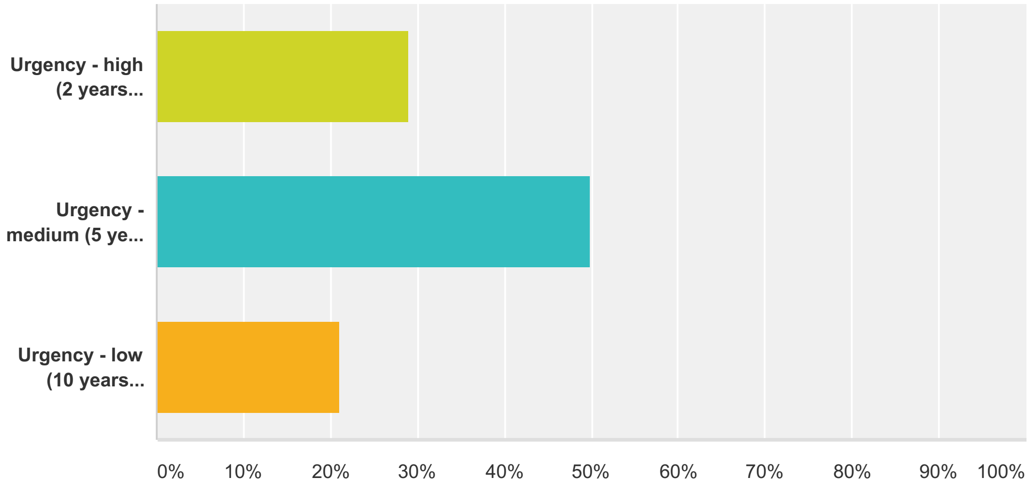
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**60.53%**	23
Urgency - medium (5 years perspective)	**31.58%**	12
Urgency - low (10 years perspective)	**7.89%**	3
Total		**38**

Q19 Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges

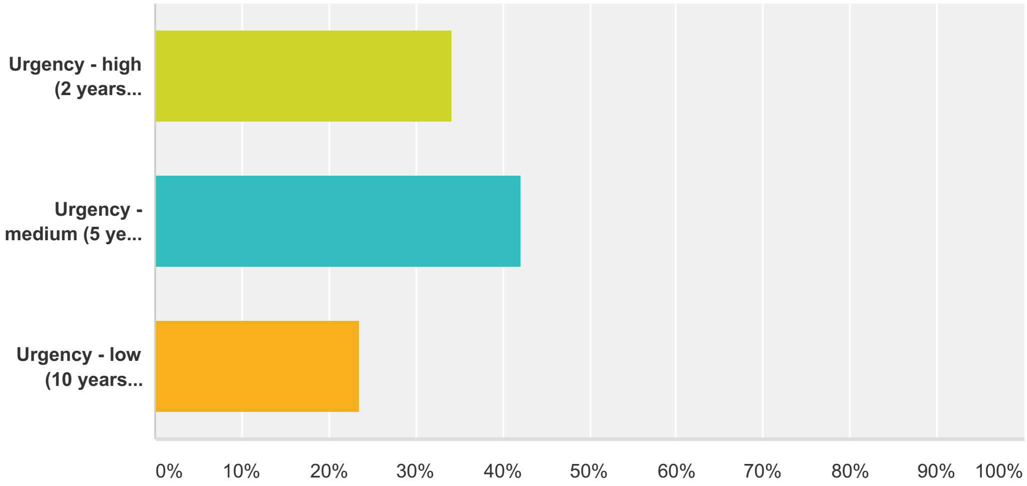
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**28.95%**	11
Urgency - medium (5 years perspective)	**50.00%**	19
Urgency - low (10 years perspective)	**21.05%**	8
Total		**38**

Q20 Promoting EU Institutional support to generic challenges and obstacles at the enterprise/ company/ SME level including incentives for cyber insurance

Answered: 38 Skipped: 1



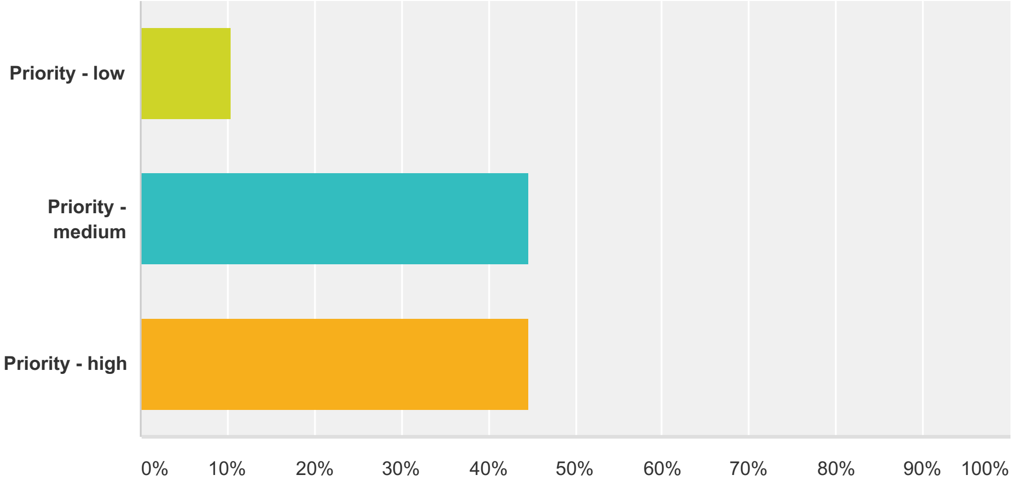
Answer Choices	Responses	
Urgency - high (2 years perspective)	34.21%	13
Urgency - medium (5 years perspective)	42.11%	16
Urgency - low (10 years perspective)	23.68%	9
Total		38

Q21 Additional Comments…

Answered: 1 Skipped: 38

Q22 Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction

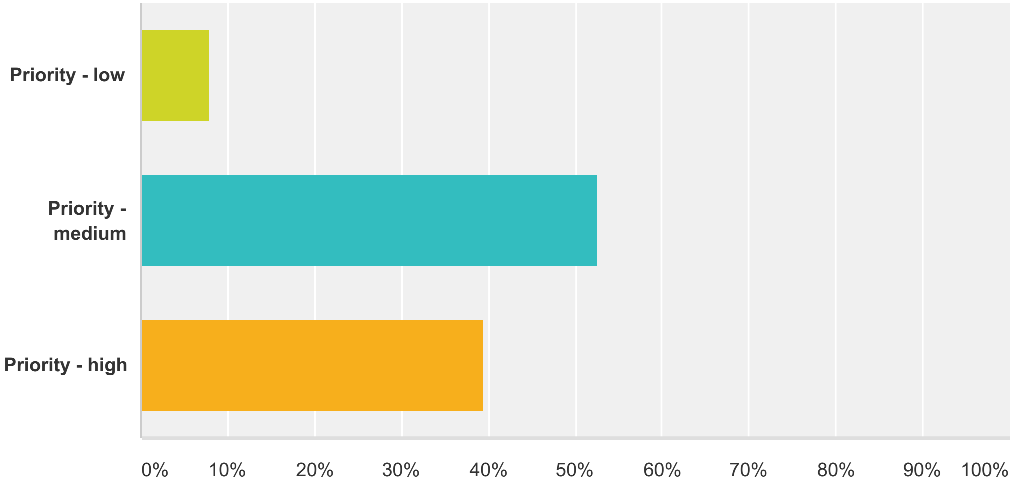
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	**10.53%**	4
Priority - medium	**44.74%**	17
Priority - high	**44.74%**	17
Total		**38**

Q23 Electronic identity and trust services for data protection across borders

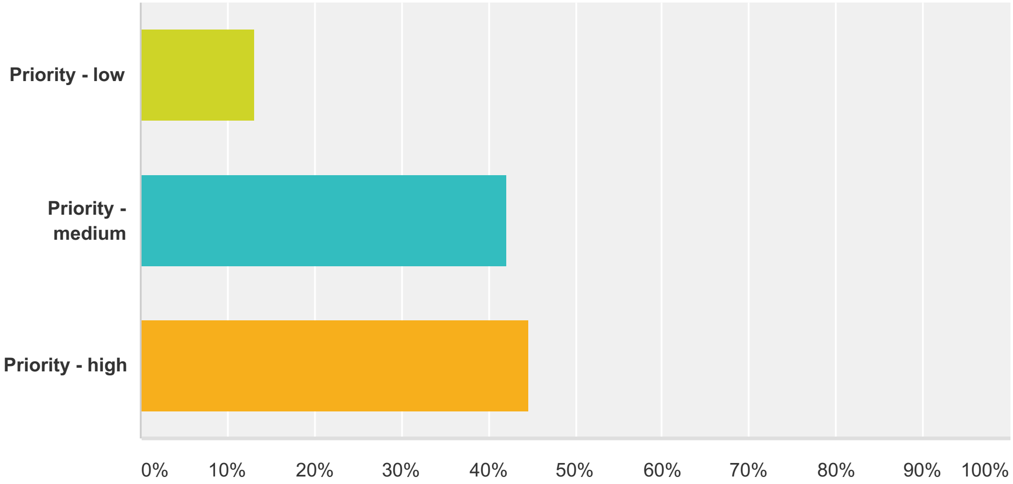
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	**7.89%**	3
Priority - medium	**52.63%**	20
Priority - high	**39.47%**	15
Total		**38**

Q24 Comprehensive legal system to fight against CC/CT

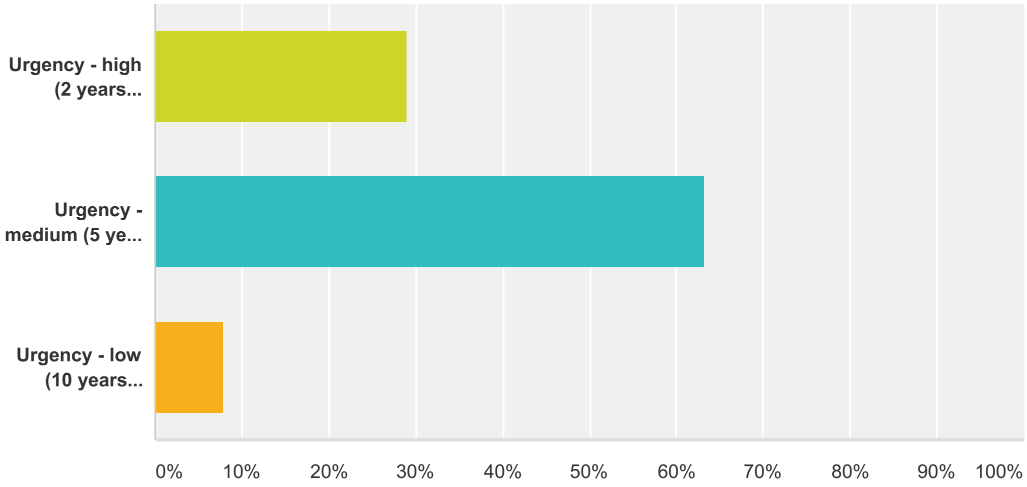
Answered: 38 Skipped: 1



Answer Choices	Responses	
Priority - low	13.16%	5
Priority - medium	42.11%	16
Priority - high	44.74%	17
Total		38

Q25 Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction

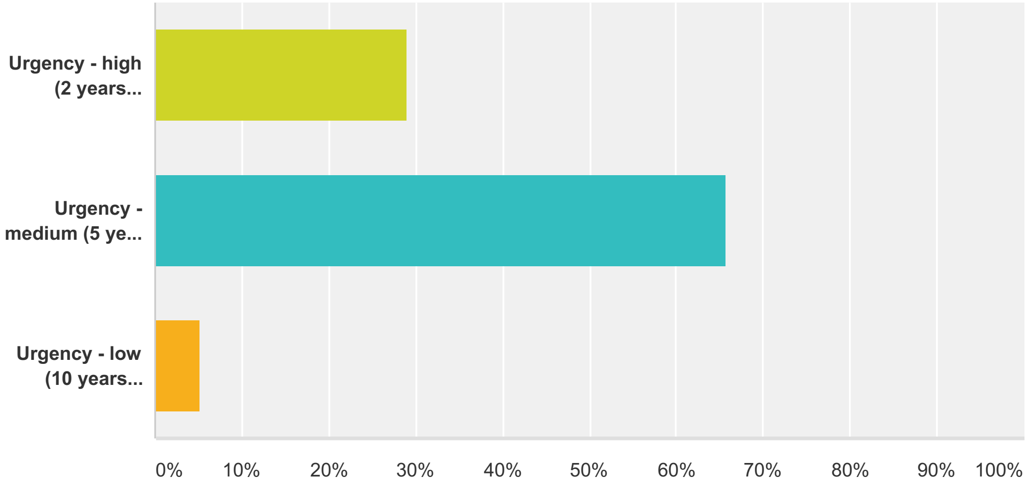
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**28.95%**	11
Urgency - medium (5 years perspective)	**63.16%**	24
Urgency - low (10 years perspective)	**7.89%**	3
Total		**38**

Q26 Electronic identity and trust services for data protection across borders

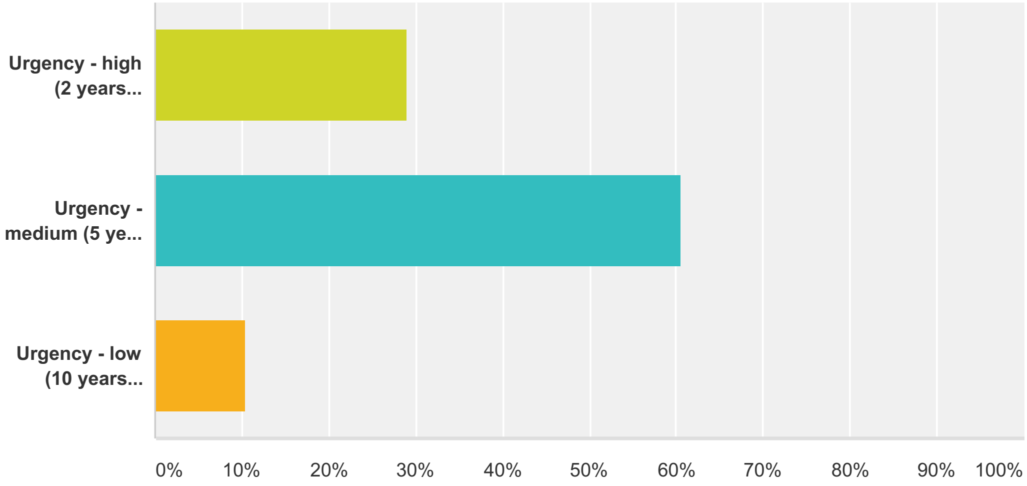
Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**28.95%**	11
Urgency - medium (5 years perspective)	**65.79%**	25
Urgency - low (10 years perspective)	**5.26%**	2
Total		**38**

Q27 Comprehensive legal system to fight against CC/CT

Answered: 38 Skipped: 1



Answer Choices	Responses	
Urgency - high (2 years perspective)	**28.95%**	11
Urgency - medium (5 years perspective)	**60.53%**	23
Urgency - low (10 years perspective)	**10.53%**	4
Total		**38**

Q28 Additional Comments…

Answered: 2 Skipped: 37

6.6 CYBERROAD-CAMINO-COURAGE WORKSHOP IN THE HAGUE - BOOKLET

CURRENT AND EMERGING CHALLENGES IN CYBERCRIME AND CYBERTERRORISM

10 - 11 MARCH 2016

NIEUWSPOORT INTERNATIONAL
PRESS CENTRE
DEN HAAG

WELCOME

It is with great pleasure that we welcome you to the Current and Emerging Trends in Cybercrime and Cyberterrorism event being held over the next two days here at the Nieuwspoort International Press Centre in Den Haag, Netherlands. The event has been organised as a cornerstone in the final stages of the COURAGE, CAMINO and CyberROAD projects, and is part of an overall thinking and knowledge exchange process to consolidate the projects' combined vision for the future of research in the fields of cybercrime and cyberterrorism across the EU.

We'd like to take this opportunity to thank all of our invited speakers, and the extended stakeholder communities surrounding each of the projects, for allowing us to draw upon your expertise and experience to help shape each of the respective research roadmaps, a process that has enabled us to address the tangible wants and needs of society within them. Presenting at the event are a selection of these individuals, who have volunteered to present to us some of their thoughts and work in tackling contemporary cyber-issues and to provide further insight into some of the challenges that we face today, and will continue to face over the coming years. The event itself aims to provide all stakeholders with a forum to exchange ideas and highlight challenges, alongside contemporaries from across Europe, so that together we can develop strategies and priorities for a common roadmap to fight cybercrime and cyberterrorism. In particular, throughout the two-day event we hope to gather insights from across Europe and beyond, to discuss further developments in the methodology, technology, and foundations for the design and effective implementation of a European roadmap for the fight against cybercrime and cyberterrorism. The event will contribute towards the development of a consolidated roadmap between COURAGE, CAMINO, and CyberRoad which will be presented to the European Commission later in 2016. This roadmap will aim to clarify the various interpretations, commonalities, and differences emanating from the European cybersecurity community as well as the results of the three projects, thereby paving the way for a more structured and well-founded approach to future research initiatives. In this booklet we'd like to introduce to you each of the projects, our efforts to develop to a consolidated approach to defining future research priorities, as well as providing an introduction to each of our invited speakers and the agenda for our event over the next two days.

Prof. Babak Akhgar
on behalf of the COURAGE, CAMINO and CyberRoad projects

CENTRIC

Centre of Excellence in Terrorism,
Resilience, Intelligence and
Organised Crime Research

AGENDA

OUR PLAN FOR THE NEXT TWO DAYS

THURSDAY 10.03.2016

13:30 14:00	Registration and Coffee
14:00 14:05	Welcome/introduction Gabriela Bodea, TNO
14:05 14:45	Keynote speech Raoul Chiesa, Security Brokers Italy *"Cyber Terrorism: wrong assumptions & true facts: what I hope will never happen"*

SESSION 1 LAW AND LAW ENFORCEMENT (NEEDS, CHALLENGES, SOLUTIONS AND PRACTICE)

Moderator Cormac Callanan (Aconite)

14:45 15:05	DI Geoff Halpin Yorkshire and Humberside Regional Cybercrime Unit
15:05 15:25	Pim Takkenberg TNO
15:25 15:45	Jerzy Kosinski WSPolSzczytno –Higher School of the Police
15:45 16:05	Judyta Kasperkiewicz University of Silesia in Katowice, Faculty of Law and Administration, Department of Forensic Science
16:05 16:15	Q&A
16:15 16:30	Coffee Break

SESSION 2 SOLUTIONS FOR THE FUTURE: COURAGE-CAMINO-CYBERROAD IDEAS

16:30 18:00 *Working session with audience*

Babak Akhgar
representative of project COURAGE

Michal Choras
representative of project CAMINO

Davide Ariu
representative of project CyberROAD

18:00 19:00 Networking reception

FRIDAY 11.03.2016

SESSION 3 CITIZENS, ENTERPRISE AND PRIVATE INDUSTRY (NEEDS, CHALLENGES, SOLUTIONS AND PRACTICE)

Moderator Davide Ariu (University of Cagliari)

09:30 09:50	Gary Hibberd Agenci UK
09:50 10:10	Rocco Mammoliti & Massimiliano Aschi Poste Italiane
10:10 10:30	Dimitris Kavallieros & Christoforos Ntantogian KEMEA/UINFC2 Project
10:30 10:45	Q&A
10:45 11:15	Coffee Break

SESSION 4 GOVERNMENT, POLICY, STRATEGIES AND AWARENESS RAISING

Moderator Luigi Rebuffi (EOS)

11:15 11:35	Quentin Revell UK Home Office Centre for Applied Science and Technology

11:35 11:55 Robin de Haas
The Hague Security Delta

11:55 12:15 Stuart Hyde
CCL Group Ltd UK

12:15 12:35 Olivier Burgersdijk
EC3/Europol

12:35 12:45 Q&A

12:45 13:45 Lunch

SESSION 5 EMERGING TECHNOLOGIES AND SOLUTIONS (INCLUDING LEGAL CONSIDERATIONS, BEST PRACTICES ETC.)

Moderator Michal Choras (ITTI)

13:45 14:05 Dr Argyro Karanasiou
BournemouthUniversity

14:05 14:25 Prof Dr. Bert-Jaap Koops

Professor of regulation and technology,
Tilburg University

14:25 14:45 Prof Wojciech Mazurczyk
Fern University and PW, Warsaw

14:45 14:55 Q&A

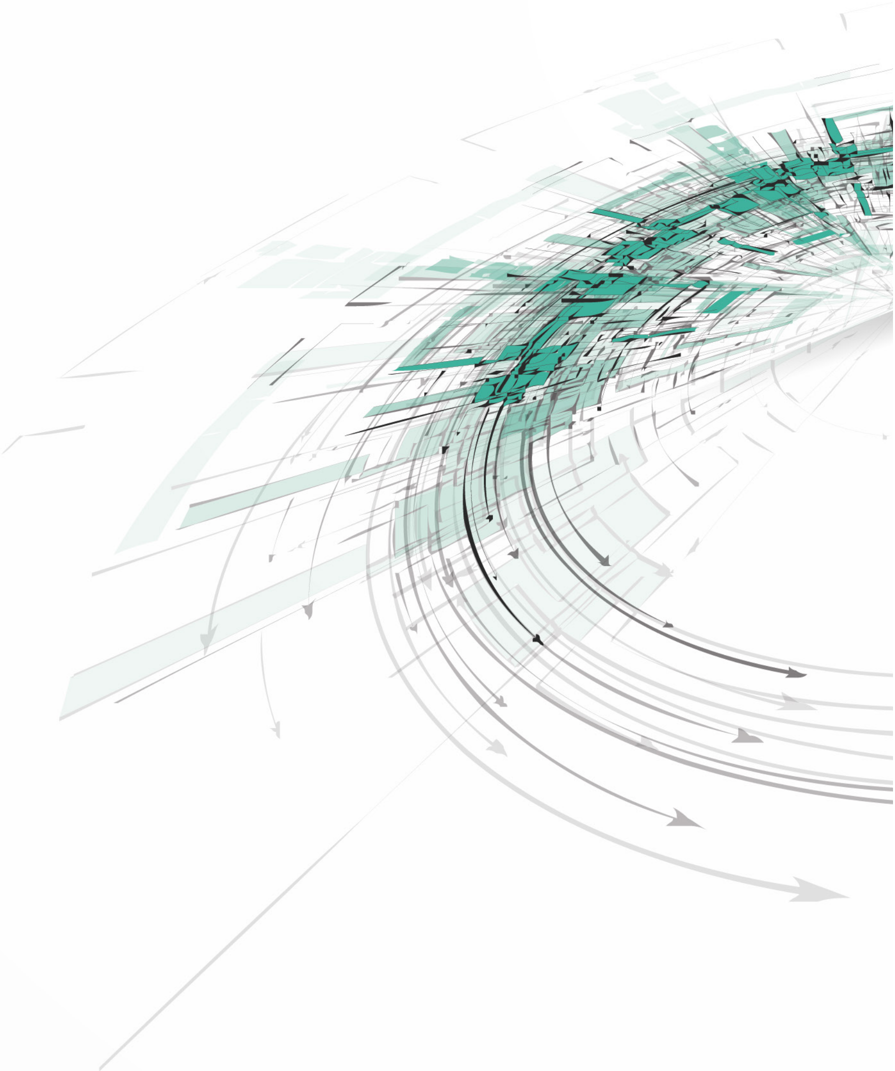
14:55 15:05 Coffee Break

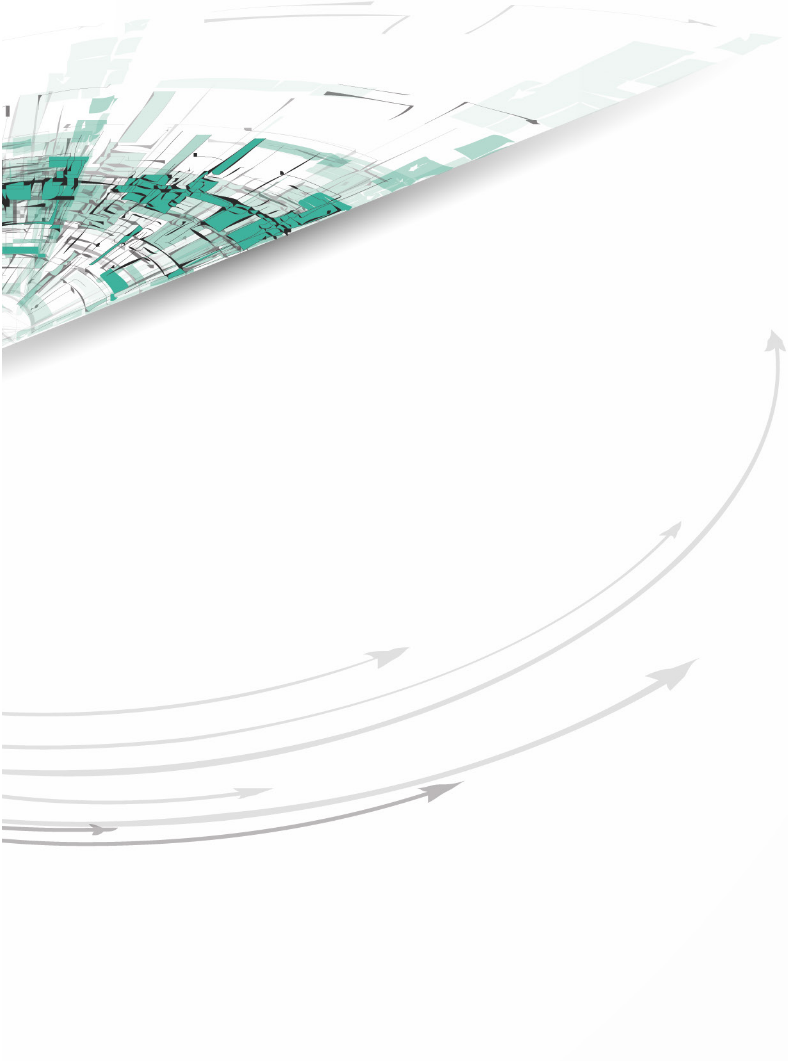
15:05 16:00 *Wrap-up and final Q&A*

Babak Akhgar
representative of project COURAGE

Michal Choras
representative of project CAMINO

Davide Ariu
representative of project CyberROAD





SPEAKERS

MEET OUR SPEAKERS

DR. ARGYRO KARANASIOU

Dr Argyro Karanasiou is an Associate Professor (Senior Lecturer) specialising in IT and Media Law, affiliated with the Centre for Intellectual Property, Policy & Management (CIPPM) and with the Data Science Institute (DSI) at Bournemouth University (United Kingdom). She is also affiliate faculty staff of Harvard Law School (2014-now), responsible for the course CopyrightX: CIPPM in the UK. Currently, Argyro is involved in media related projects with the Council of Europe (Regional Expert on online media and reconciliation in South Eastern Europe) and with the OSCE Representative on Freedom of the Media. Recently (Jan 2016), Argyro was invited to join the EFF's group of experts on Free Trade Agreements and Digital Services, providing expertise on how TISA and TTIP will affect online consumers in the EU. In 2013 (Indonesia) and 2015 (Brazil), she was awarded an Internet Society IGF Ambassadorship and in 2014 she was named a PhD Ambassador by the Information and Privacy Commissioner in Ontario, Canada. Her research discusses techno-legal conceptual frameworks for decentralised internet regulation with a particular focus on free speech, data protection, media ownership, and user empowerment. Her current projects span a wide range of topics from IoT/wearable tech to big data and mesh networks. Argyro tweets @ArKaranasiou on all things tech.

PROF. BABAK AKHGAR

Prof Babak Akhgar is Professor of Informatics and Director of CENTRIC (Centre of excellence in terrorism, resilience, intelligence and organised crime research) at Sheffield Hallam University and Fellow of the British Computer Society. He gained considerable commercial experience as a strategy analyst and methodology director for several international companies. Prof. Akhgar has more than 100 referred publications in international journals and conferences on information systems with specific focus on knowledge management and its application with contemporary security contexts (e.g. Application of social media in crisis management, intelligence based combating of terrorism and organised crime, gun crime, cyber security, public order and cross cultural ideology polarisation). He is technical coordinator of the COURAGE project.

PROF. BERT-JAAP KOOPS

Bert-Jaap Koops researches the interaction between technology and law, in particular criminal law and regulation issues. His main research fields are cybercrime, cyber-investigation, privacy, and data protection. He is also interested in topics such as DNA forensics, identity, digital constitutional rights, 'code as law', and regulatory implications of human enhancement, genetics, robotics, and neuroscience. With a personal postdoc (1999), VIDI (2003) and VICI

(2014) grant, Koops is one of the few Dutch researchers who received all three stages of NWO's (Netherlands Organisation for Scientific Research) personal research-grant scheme. From 2005-2010, he was a member of De Jonge Akademie, a young-researcher branch of the Royal Netherlands Academy of Arts and Sciences https://www.tilburguniversity.edu/webwijs/show/e.j.koops/. He is currently working on the COURAGE project.

DR. CHRISTOFOROS NTANTOGIAN

Dr. Christoforos Ntantogian received his B.Sc degree in Computer Science and Telecommunications in 2004 and his M.Sc degree in Computer Systems Technology in 2006 both from the Department of Informatics and Telecommunications of University of Athens. In 2009 he received his Ph.D. from the University of Athens (Department of Informatics and Telecommunications). Currently, he is an adjunct lecturer and senior researcher at the Department of Digital Systems of the University of Piraeus. Dr. Christoforos Ntantogian has participated in numerous projects realized in the context of EU Programs (e.g., CONTENT, ANA, CASCADAS). His research interests lie in the intersection of data analysis, applied mathematics and system/software security to develop practical systems with security intelligence. Christoforos currently works on the UINFC2 Project.

CORMAC CALLANAN

Cormac Callanan owns/operates an independent consultancy company from Dublin, Ireland called Aconite Internet Solutions (www.aconite.com) which provides expertise in policy development in the speciality area of international cybercrime and Internet security & safety. Qualified in Computer Science he has over 25 years working experience on international computer networks and 15 years' experience in the policy area of illegal content andcybercrime activities on the Internet. He was co-author of the Council of Europe Guidelines on Cooperation between Law Enforcement and Internet Service Providers quoted by the European Court of Human Rights as achieving the appropriate balance between sharing data and data protection. He is a member of the Irish Internet Safety Advisory Committee reporting to the Irish Department of Justice. He has provided training at Interpol and Europol and to law enforcement agencies around the world on the subject of emerging and developing technologies, cybercrime and the role of internet industry. Cormac is currently working on the COURAGE project.

DR. DAVIDE ARIU

Davide Ariu holds a research assistant positionat University of Cagliari, workingwith the Pattern Recognition and Application Lab (http://pralab.diee.unica.it). He has a background on Pattern Recognition and Machine Learning applications to Computer Security, having obtaineda Ph.D. in Computer Security in 2010. In 2007 he has beenvisiting Scholar at the Georgia Tech Information Security Center in Atlanta (U.S.).He has currently published 20 papers on peer-reviewedinternational journals, conferences, and workshops.He is one of the lecturers of the Computer Security course at the Department of Electronic Engineering, and is also among the organisers of Building Trust in the Information Age, a summer school on Computer Security and Privacy. Within PRA Lab Davide Ariu is also responsible for coordinating the activities concerningthe participation ofthe Lab in European, national, and regional projects. Currently, he is the project manager of the European projects DOGANA and CyberROAD. Formerly, he has been the manager of the projects ILLBuster and MAVEN, and of the regional project sTATAIn 2015 he co-founded PLURIBUS ONE (https://www.pluribus-one.it), a research intensive spin-off of the University of Cagliari.

DIMITRIOS KAVALLIEROS

Dimitrios Kavallieros holds a BSc in Information Management and an MSc in Ethical Hacking and Computer Security. He has held previous posts as a Network/System Administrator in Pentelis Childrens Hospital, Programmer in Computer Solution SA. Since 2014 he has worked as a Research Associate at the Center for Security Studies (KEMEA), highly involved in European and National Research Programmes mainly focused in Cloud Security, Cybersecurity/ Cybercrime and the relevant Ethical, Legal and Societal impact. Dimitris is currently working on the UINFC2 Project.

GABRIELA BODEA

Gabriela Bodea is senior policy researcher with TNO. Her area of research is the social impact of ICT. She specializes in privacy in relation to information and communication technologies, and in particular in relation to various aspects of e-Government (such as electronic authentication, homeland security, identity management); the future internet; and emerging and converging technologies. Gabriela currently works on the COURAGE project as part of her role at TNO.

GARY HIBBERD

Gary was appointed as Managing Director of Agenci Information Security in 2012 but began his careeras an IT programmer back in 1985 and has had a passion for all things cyber related since then. His broad range of experience in almost every discipline in IT means he knows ‘What good looks like’ when it comes to protecting your business and reputation.He is a published author, experiencedand qualified in Information Security & Business Continuity who is a passionatespeaker on cyber security and related disciplines. He is regularly asked to present at conferences and schools to helpraise awareness and understanding of real world, business related issues affected by our digital world.Gary has helped businesses as diverse as the RSPCA to LateRooms.com to improve their security and recovery capabilities a cross the world and held the role of European Crisis Management Leader for GE Money.

DI. GEOFF HALPIN

Geoff is the Detective Inspector leading the police Regional Cyber Crime Unit which forms part of the Yorkshire & Humber Regional Organised Crime Unit, and is recognised as one of the leading experts on cybercrime law enforcement in the UK. He leads a team of specially trained officers and staff working with partners in law enforcement, industry and academia to investigate and prevent the most serious incidents of cyber-crime at a regional, national and international level. He came to law enforcement from an academic background, having studied computing at university including security, artificial intelligence and neural networking/ pattern recognition. He has over 20 years’experience as a police officer in Nottinghamshire, West Yorkshire and at the Regional Organised Crime Unit working in a variety of specialisms including homicide investigation, serious and organised crime, intelligence and cyber-crime. He has a particular interest in the use of computers for predictive policing including crime and disorder prevention, and intelligence development.

LT. COL. JERZY KOSIŃSKI

Lt Col Jerzy Kosiński, PhD Eng - professor at the Institute for Research on Crime and Terrorism, Police Academy in Szczytno. His scientific specialties are cybercrime and digital evidence. He was previously a member of Interpol and Europol expert groups on cybercrime. He has organised a series of cyclic international scientific conferences addressing the "Technical aspects of ICT crime", "Electronic payment instruments abuses" and "IPR crime in Internet". Author of numerous publications and presentations at conferences in the field of their specialization in science, J. Kosiński is also an expert witness in the cybercrime area.

JUDYTA KASPERKIEWICZ

Judyta Kasperkiewicz is a Polish advocate and Ph.D. candidate at Silesia University in Katowice, Poland. She specializes in cybersecurity and intellectual property law. She has substantial experience in criminal, civil and family law gained in Poland and the United Kingdom. She is a publisher of reviewed academic articles in law. She lives in New York.

LUIGI REBUFFI

Luigi Rebuffi has been with EOS ever since its creation in 2007. Having proposed and launched the initial idea of EOS in 2003, he now plays a strategic role in defining the mission and objectives of EOS; coordinates the implementation of the agreed strategy with Members and Partners; and supports and advises the EOS Members. Mr Rebuffi leads EOS' comprehensive advocacy approach and plays a key role promoting public–private cooperation on security in coordination with the activities of ASD and EOS Members. He ensures the effective and efficient implementation of projects, directs and manages the EOS team, and has a decisive impact in influencing EU policy-making in security through communication with the European Institutions at the highest level. In this capacity, he is an advisor on security issues to the Cabinets of several EC Commissioners, is a Member of the Security Advisory Group on EU Security Research of DG ENTR and is President of the Steering Committee for security research of the French ANR (National Research Agency). Having a background in nuclear engineering, before EOS he worked in different positions at ITER, Thomson CSF, and Thales.

DR. MICHAL CHORAS

Michal Choras obtained his Doctor of Science (habilitation) degree in computer science from AGH Cracow in 2014. Since 2015 he holds the professor position at University of Science and Technology (UTP) in Bydgoszcz, where he is the Chair of Teleinformatics Systems Division. Earlier, he obtained M.Sc. and PhD in telecommunications from UTP in Bydgoszcz in 2002 and 2005, respectively. He also works as consultant and project manager at ITTI Sp. z o. o.

His interests include cyber security, information management and pattern recognition in several domains, such as image processing, security (network security, urban security, and biometrics) and safety (crisis management, critical infrastructures). He has been involved in EU FP7 projects (e.g. INTERSECTION, INSPIRE, TACTICS, CIPRNet) and EDA projects (e.g. ATHENA). Currently, he is the coordinator of FP7 project CAMINO (www.fp7-camino.eu) on cybercrime and cyberterrorism. He is an author of over 150 reviewed scientific publications, including a number of publications regarding methods for cyber security, pattern recognition, image processing and security/safety applications. He is also a reviewer and Programme Committee member for over 35 journals and over 35 conferences. Currently, he is a vice-chair of IMG-S Thematic Area 7 on cyber security.

OLIVIER BURGERSDIJK

Olivier is currently head of strategy for the European Cybercrime Centre (EC3). After completing his university education (Criminology), Olivier Burgersdijk joined the Rotterdam-Rijnmond police force in The Netherlands (1998-2001), where he was active in the areas of conducting evaluations on major criminal investigations of serious and organised crime, as well as strategic analysis. From 2001 to 2006 Mr Burgersdijk supported as consultant various regional police forces and prosecution services in The Netherlands in the areas of quality management, evaluation and information management. From 2006 till present Mr Burgersdijk is active within Europol in different functions with responsibilities for information exchange and information management at strategic as well as technical levels. Since November 2012, he has held the post of Head of Strategy within the European Cybercrime Centre, overseeing strategic analysis, outreach, expertise, R&D, specialised forensic tools & techniques.

PIM TAKKENBERG

Since 2014 Pim Takkenberg has held the position of Cyber Security director with Northwave. Mr. Takkenberg graduated from the high-grade Master's Programme in Police Leadership in 1999. In 2011 he graduated from the FBI National Academy (247). In 2006, Mr. Takkenberg joined the Dutch National High Tech Crime Unit (NHTCU). As head of the NHTCU, Mr Takkenberg was responsible for a unit dedicated to investigating advanced and organized forms of cybercrime. Successful cases conducted by the unit include the Bredolab Botnet takedown, the investigation of DigiNotar hack, and the investigation of the hacking of major telecommunication company KPN. In 2013, Mr. Takkenberg joined the Ministry of Interior and Kingdom Relations as head of the Cyber Intelligence Team (CIT). The CIT conducts investigations into digital attacks containing an aspect of cyber espionage or cyber sabotage, carried out primarily by state actors, and which in turn form a threat to Dutch national security and economy.

QUENTIN REVELL

Quentin has worked for the UK Home Office since 2001 developing technical surveillance tools and methods. Quentin has lead the development and support of a national GIS system - used for countering serious and organised crime. From 2010 he managed the Home Office - Biometric Centre of Expertise and supported the Home Office's Senior Biometric Advisor to provide horizon scanning and technical assurance to the Home Office and across UK government / international partners. His research helped establish Centre for Applied Science and Technology (CAST) as a leader in understanding the use of automatic facial recognition from CCTV, and the issues of facial comparison. More recently Quentin has moved to work on Digital Investigations area and lead their Open Source Investigations programme. This programme brings together his knowledge of identity and surveillance to assure the Home Office that its use of Open Source Investigations across all of its priority areas (to Prevent terrorism, Cut crime and Control immigration) is Safe, Legal, Effective and efficient - now and into the future.

RAOUL CHIESA

Raoul Chiesa was born in Torino, Italy. After being among the first Italian hackers back in the 80's and 90's (1986-1995), Raoul decided to move to professional InfoSec, establishing back in 1997 the very first vendor-neutral Italian security advisory company; he then left it in 2012, and established along with former and new partners "The Security Brokers", a visionary joined stock company providing niche, cutting-edge security consulting services and solutions. Raoul is among the founder members of CLUSIT (Italian Information Security Association, est. 2000) and he is a Board of Directors member at ISECOM, OWASP Italian Chapter, and at the Italian Privacy Observatory (AIP/OPSI); he has been one of the coordinators of the Working Group "Cyber World" at the Center for Defence Higher Studies (CASD) between 2010 and 2013 at the National Security Observatory (OSN) at Italy's MoD. He is a former member of the ENISA Permanent Stakeholders Group (2010-2012 and 2013-2015), an independent "Special Advisor on Cybercrime and Hacker's Profiling" at the UN agency UNICRI, and a Member of the

Coordination Group and Scientific Committee of APWG European chapter, the Anti-Phishing Working Group, acting like a "Cultural Attachè" for Italy. Since July 2015 he's a Board Member at AIIC, Italian Experts Association on Critical Infrastructures, a Subject Expert for ADETEF (different French ministries) at ENCYSEC (Enhancing Cyber Security), a project funded by the European Union, and a member of the ITU (UN-Geneva) Roster of Experts on Cybersecurity. Raoul publishes books, white papers and articles worldwide, which are often translated in different languages (English, French, Italian, Romanian, Spanish, Chinese) as main author or contributor, while being since more than 20 years a worldwide known and appreciated Key Noter and Speaker; giving all of the above, Raoul is a regular contact for worldwide medias (newspapers, TV, radio, podcasts and bloggers) when dealing with Information Security issues, ICT security incidents and IT trends.

ROBIN DE HAAS

Robin de Haas is Program Manager for the Hague Security Delta. After getting a Master of Business Administration with a specialization in Change Management, Robin served in the Dutch Army as an officer during military service. After this he joined Randstad for three years and worked as an intermediary between businesses and personnel. Robin worked for 17 years at TNO Defence, Safety and Security as program manager for the Next Generation Combat Aircraft and the Replacement F-16 program. His involvement with the Hague Security Delta started in 2007 working as program manager of the Secure Haven project. This project worked out scenario's and blueprints for the municipality of The Hague to become a city that combines economy and security and is nice to live and work in. He was head of the department Networked Organizations which has expertise on Crisis management, Critical Infrastructures, Urban Security and Cyber Security. Robin has been responsible since 2011 for the development of TNO's cyber security R&D portfolio. As a program manager at The Hague Security Delta his main focus area is creating and stimulating triple helix cooperation between government, businesses and knowledge institutes in the field of Cyber- National- and Urban Security.

ROCCO MAMMOLITI

Rocco Mammoliti has over 15 years of experience in the information security industry and has also carried out research and innovation in information engineering and biomedicine. He is the author of several scientific publications on topics related to modelling, data mining, and ICT security as well as on issues of innovation and new technologies. He has worked for companies of significant importance in the field of IT and telecommunications industries such as Bull and Telecom Italy, covering in time the roles of Head of IT Security and Chief Information Security Officer. He is a member of international professional associations including the IEEE and the Computer Society. His main areas of expertise are related to domains in the Network & Information Security, creation and management of SOC (Security Operations Center) and CERT (Computer Emergency Response Team), Abuse & Cybercrime Prevention, Child Online Protection, etc. He is currently Head of Security function of Poste Italiane, in which he oversaw the creation of the Italian Post Office CERT. He holds the position of Technical Manager of Scientific-Technological District Cyber Security and General Manager of GCSEC Foundation (Global Cyber Security Center), of which the Italian Post Office is a founding member.

STUART HYDE

Stuart Hyde QPM has Completed a full career within the Police service in the UK with Exemplary Service and national recognition through the awarding of the prestigious Queens Police Medal and presentation of an Honorary Doctorate for commitment to Cybercrime prevention and detection. Director of Stuart Hyde Associates and spokesperson on a range of technical and cyber issues supporting a number of individuals and organisations with specific Digital Forensic, Cybercrime and personal consultancy. He has a unique understanding of national strategic and operational tactical understanding to help create effective improvements and solutions.As a member of the Europol Internet Security Advisory Board and Vice President of two Not for Profit organisations he is ideally placed to add value to any debate on Cybercrime. He is a Director of Solutions for CCL Digital Forensics and an Associate for the innovative Cybx cyber Exercise training facility at the Emergency Planning College.He runs Stuart Hyde Associates and has developed the concept of Digital Leader to address the lack of cyber and digital knowledge amongst senior and middle managers.

DR. WOJCIECH MAZURCZYK

Wojciech Mazurczyk received his B.Sc., M.Sc., Ph.D. (Hons.), and D.Sc. (Habilitation) degrees in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland, in 2003, 2004, 2009, and 2014, respectively. He is currently an Associate Professor with the Institute of Telecommunications, WUT, where he is the Head of the Bio-Inspired Security Research Group and a Researcher at the Parallelism and VLSI Group at Faculty of Mathematics and Computer Science at Fern Universitat, Germany. He is an author or co-author of over 100 papers and over 30 invited talks devoted mainly to network security. His research interests include bioinspired cybersecurity and networking, information hiding, and network security. He is involved in the technical program committee of many international conferences, including the IEEE INFOCOM, the IEEE GLOBECOM, the IEEE ICC, and ACSAC. He also serves as a reviewer for major International magazines and journals. Since 2013, he has been an Associate Technical Editor of the IEEE Communications Magazine (IEEE Comsoc) and an IEEE Senior Member.

CONSOLIDATED RESEARCH AGENDA

OUR COMBINED VISION FOR THE FUTURE OF CYBERCRIME RESEARCH

In response to suggestions made at the joint first review meeting of the CAMINO, COURAGE and CyberROAD projects, held at the offices of the European Commission, Brussels on June 4th 2015, the three consortia have undertaken to consolidate each of their respective outputs into a single, unified and easily digestible research roadmap that can be distilled to inform future works, related policies and funding initiatives that address the challenges being faced by society due to the proliferation of cybercrime and the threat of cyberterrorism. Underpinning each of the existing cyber roadmap frameworks were a series of integral and interlinked dimensions. These four features; Technical, Human, Organisational, and, Regulatory, are each individually attributed to all aspects of cybersecurity strategy, resilience, and vulnerabilities. Due to the broad and complex scope of cybersecurity concerns and challenges, each research agenda items, essential research agenda item fits into at least one dimension of the THOR categorisation, however many are at least partially linked to more than one. Therefore, the THOR analysis does not propose itself to be the sole identifying means of categorization, rather as a set of key underlying factors that are flexible, dynamic and interchangeable in order to address the plethora of fluctuating contemporary European cybersecurity challenges. The following provides an overview of the topics included in the current draft of this consolidated agenda, highlighting a number of what we collectively consider to be priorities for future research and practice. We do not consider these topics to be comprehensive, and invite you to submit your own ideas throughout the conference at bit.ly/CyberRoadmap.

TECHNICAL

STRENGTHENING EMERGING TOOLS FOR BIG DATA ANALYSIS, CLOUD FORENSICS AND SECURITY

Cyber-attacks are not always immediately visible due to their nature or intensity (e.g., amount of traffic they introduce). Therefore, recently techniques using big data tools have been adapted. Recent research has shown that in depth analysis of large volumes of data (received from different segments of IT networks) has a unique capability of revealing interesting patterns. This concept can potentially be adapted and applied to many cyber-security areas, namely: spam detection, botnets detection, malwares analysis, web-based infection, network intrusion detection systems.

Dimensions (THOR)	Consolidated Roadmap			
	Technical	Human	Organisational	Regulatory
Topics	Strengthening emerging tools for big data analysis and cloud forensics and security	Collective awareness and education for increased societal resilience to CC/CT threats	Adapting organisations to the cross-border nature of the Internet and cybercrime/ terrorism	Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction
	Establishing metrics and framework for cyber security testing	New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies	Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges	Electronic identity and trust services for data protection across borders
	Countering cyber crime affecting mobile and IoT devices	Definition, characteristics and behaviors of the offenders and victims in cybercrime	Promoting EU Institutional support to generic challenges and obstacles at the enterprise/ company/SME level including incentives for cyber insurance	Comprehensive legal system to fight against CC/CT

This topic is focused particularly on the correlation of capabilities for big data analysis and scalability of big data tools and methods. The topic includes also consideration on challenges related to the realistic workload conditions of currently used test-beds that have to operate in real-time or near real-time. Moreover security of big data infrastructures is also addressed.

As a result of the recommendations given in this topic, we expect that typical network monitoring solutions will evolve to context aware systems which allow the user to identify current cyber security problems and what is more important – their roots. The second important expectation is the test beds community using wide variety of data samples (data sets) containing different malwares, real and synthetic network traffic characteristics (or other challenging problems) that will be widely available to researchers.

ESTABLISHING METRICS AND FRAMEWORKS FOR CYBER SECURITY TESTING

One of the most important and demanded aspects in every product, system or even organisations is quality; guaranteeing fundamental characteristics such as reliability or availability in any system, moreover if it is a security one, is an essential part of revealing the development team's confidence in their system or product. Therefore, activities focused on maintaining and improving this quality are needed, and the most effective ones are testing and simulation processes. Concepts such as automated tools or cyber exercises between companies will help to raise the awareness of not only cyber security responsible people, but also of the rest of the staff. And finally, in order to promote and encourage the realisation of all these necessary actions, proper regulations and standards should be made and discussed, and thus achieve a desirable and prepared environment to benefit all these good practices.

Therefore, the key points of this topic include Security-by-Design issues, development of representative security metrics, sharing of information about vulnerabilities, and building open test beds for testing cyber security. On the other hand, issues of access control and trust management in distributed environment are also addressed. Finally, the ultimate goal of development and implementation of the specified topic milestones is objectiveness and measurability of cyber security for assurance purposes.

COUNTERING CYBERCRIME AFFECTING MOBILE AND IOT DEVICES

Nowadays, one of the main challenges affecting countering cybercrime is large and still increasing amount of malware samples. Evolution and changeability of malwares and botnets (e.g. new, fast-evolving botnet architectures) are also factors that should be addressed by the research communities to more effectively fight against cybercrime. This is particularly important in the context of limitations of existing signature-based scanners and malware detectors. On the other hand, cybercrime affects also mobile devices, and in the near future will affect micro devices (now not often connected to the Internet), that will be exposed to cyberattacks in conjunction with growing popularity of IoT (Internet of Things) concept.

Primarily, this topic focuses on development of new paradigms for fighting against malware targeting mobile and small/micro devices, including new ways to counter evolving and robust botnets and their detection. Investment in large-scale (even Internet-scale) testing environment is also one of the points addressed in this topic, due to the need for prediction of botnet evolvement, safe observation of malware spreading directions and timing, as well as setting up the most effective containment strategies.

HUMAN

COLLECTIVE AWARENESS AND EDUCATION FOR INCREASED SOCIETAL RESILIENCE TO CC/CT THREATS

This topic focuses on the identification and facilitation of new approaches to enable the increased resilience of society to cyber-security threats through increasing the awareness and education levels of stakeholders across society; ranging from citizens through to security professionals, policy makers and the full spectrum of private sector and critical infrastructure providers. Prevention strategies, and in this context, particularly those associated with increasing awareness and standards related to online safety and information security play an important role in improving societal resilience to cybercrime, while 'human security' specifically is an import factor as popular attack vectors such as social engineering and phishing continue to exploit human security vulnerabilities.

Under this topic research should focus on the identification of new approaches to increasing societal awareness, and subsequently readiness, to deal with cybersecurity threats and thus cybercrime. Where necessary, the impact of new and emerging technologies and behavioural changes that occur because of them should be identified and considered. The research proposed should identify and address awareness and education requirements across levels and sectors, such as national teaching curricula, law enforcement and other public and private sector institutions.

NEW STANDARDS FOR PRIVATE DATA MINIMISATION, APPROPRIATE USE AND RE-USE OF DATA AND PRIVACY ENHANCING TECHNOLOGIES

With surveillance powers and techniques a very current topic, both from the perceived excessive use in some quarters and the inadequate interpretation of available evidence in others, the roadmap towards more effective implementation of Privacy Enhancing Technologies is inexorably entwined with the development of forthcoming legislation, and the regulatory interpretation of these. In particular DPR, eIDAS, and Payment Services Directive 2's early adoption through SecuRe Pay, introduce requirements for the adoption of PETs (Privacy Enhancing Technologies), albeit through the adoption of undetermined techniques or technologies, even in advance of their formal ratification into EU or Member State legislation. These advance regulatory roadmaps provide an interesting, and often unexpected, set of requirements to the organisations handling sensitive personal data.

Other issue raised in this topic is the fact that under a range of current regulations and industry standards, across a wide and varied range of industries, the use of data is frequently, but not universally, restricted to the use originally intended when data was collected. Users also face a range of opt-ins or opt-outs to the use, or subsequent re-use, of this data. The advent of big data has made the search for new uses of data held on existing systems a growth industry, but there are strong Human and Ethical concerns raised through this re-use. The application of these existing data sets for LEA purposes has caused some debate, and our Roadmap will provide pointers to those issues that need to be addressed and to what timescale.

DEFINITION, CHARACTERISTICS AND BEHAVIOURS OF THE OFFENDERS AND VICTIMS IN CYBERCRIME

The scale and profilieration of Internet use as a means to facilitate crime has also introduced new challenges for the social and behavioural sciences, in addition to the technological and criminological disciplines we normally associate with studies in the domain. Due to the potential overlaps and absences of clarity in distinguishing between cybercrime, cyberterrorism, cyber warfare, and often the inability to immediately identify the origin of an attack means that there is significant benefit in assessing the impact of an attack and discerning the potential motivations behind it. The enormous widespread impact exerted by modern cybercrime means that individuals and groups involved in committing, responding to, and, preventing events, is equally expansive. The sheer quantity and diversity of the number of criminals and victims of cybercrime means that despite the importance of analysing the various different actors, there has been little progress to date.

In order to develop and deliver improve intervention and prevention measures, this research topic proposes research to help build our understanding of the diverse range of actors involved. Research has shown that cybercrime is no longer the reserve of technically skilled individuals and groups, so more work is need to establish the underlying factors that contribute to the profiles of victims and offenders a like, in addition to establishing human, environmental and other PESTLE factors that drive cybercrime.

ORGANISATIONAL

ADAPTING ORGANISATIONS TO THE CROSS-BORDER NATURE OF THE INTERNET AND CYBERCRIME/ TERRORISM

Nowadays, competitiveness is global, so any company or system can receive an attack from anywhere on the planet. Therefore, it is vitally important that regulatory differences between countries are known and understood, and in consequence organisations should be aware of this fact and protect their assets and intellectual property taking this into account. Organisations need to adapt to think, protect their systems and networks, and cooperate without borders. Therefore, key research points of this topic concern homogenisation of law, cooperation between Law Enforcement Agencies (LEAs), CERTs, governmental cooperation in terms of cross-border monitoring and information sharing. Top priority milestones include also interoperability of forensic, in particular tools and best practices.

CREATING USER-FRIENDLY TERMINOLOGY, LANGUAGE AND FEATURES TO ASSURE A BETTER UNDERSTANDING OF CYBER SECURITY CHALLENGES

The definitions and understanding of terminology used in reference to cybercrime and cyberterrorism are, in some instances, inconsistent across EU Member States, potentially causing confusion and in extreme cases hinder law enforcement, prosecution and international cooperation efforts due to the ambiguity surrounding the subject area in general. Harmonising terminology in both areas of cybercrime and cyberterrorism is crucially important in defining how the LEA sector should cooperate in an EU and broader international context. Without a clear understanding of the characteristics that distinguish them, these areas will be hard to addresses properly across all relevant levels. The absence of equal representation and understanding of terms from both areas of cybercrime and cyberterrorism, the lack of definition of terms and the different taxonomy in current use in the field is identified as a problem by academia, LEAs, and by entities representing legal and ethical organisations as well as from the critical infrastructure stakeholders.

In this topic, it is proposed that efforts must be made to increase levels of knowledge exchange among stakeholders, leading to the provision of harmonised and standardised terms through the development of a new taxonomy framework that involves all aspects of cybercrime and cyberterrorism, specifying their differences and commonalities.

PROMOTING EU INSTITUTIONAL SUPPORT TO GENERIC CHALLENGES AND OBSTACLES AT THE ENTERPRISE/ COMPANY/ SME LEVEL INCLUDING INCENTIVES FOR CYBER INSURANCE

Common / unified institutional support is needed to promote changes at the Enterprise, company and SME levels. The creation of an expert committee at the request of the main involved countries can contribute to overcoming these obstacles and challenges at a European level. In addition, an information sharing platform can help the approach and collaboration between interested parties, making quick and efficient ideas/problems sharing possible. This support will assure the minimum protection needed in these organisations.

On the other hand, it is widely accepted that achieving perfect security is impossible. Security accidents and data breaches will occur regardless the amount of security controls and practices applied (though with much lower frequency). Thus, organisations have to deal with the residual risk. Recently, insurance, a usual treatment approach for residual risk, was applied to the cyber world. The developing cyber insurance market faces a number of unique as well as usual (for insurance) challenges. In particular, heavy information asymmetry, lack of statistical data, interconnected security and correlated risks, rapid change of risk landscape, unclear underwriting language, etc.

REGULATORY

DEALING WITH DIFFERENT LEVELS OF LEGAL FRAMEWORKS FOR ILLEGAL CONTENT: QUESTIONS OF GEOLOCATION AND JURISDICTION

Cybercrime is inherently a cross border issue, potentially involving a number of different countries and territories each with their own legal frameworks and jurisdictions. This 'internationalisation' of crime creates new challenges for law enforcement. This includes issues such as the reporting and deletion of illegal content, the collection of court evidence, cross-border accessibility of data and other issues.

In this research topic, the identification and development of new methods that enable LEAs to gather and share information across geographic borders resulting in improved cross border cooperation among international and public/private authorities and to support the development of new standards for harmonising collaboration between the private sector and law enforcement.

ELECTRONIC IDENTITY AND TRUST SERVICES FOR DATA PROTECTION ACROSS BORDERS

The research community will need to address the technical standards to be agreed for the degrees of identity and authentication, and the circumstances under which each is appropriate. The research community will play a vital role in this area as what is perceived to be 'uncrackable' in some Member States (or nations outside the European Union) could have relatively trivial flaws when looked at from outside. A majority of classes and applications of Cybercrime and Terrorism contain a misrepresentation of identity or attempt to authenticate access to goods or services that the attacker has no legitimate use for. Currently a plethora of standards exists that enable the identification and authentication of genuine users. At present there is no interoperability of these, and poor controls over the degree to what constitutes 'strong authentication' sufficient for each respective application.

The proposed research identified in this topic includes the timetable for the implementation of eIDentity, Authentication & Signature regulations, and the steps necessary to ensure its impact internationally. Equally, with the payments industry now being required to look at early adoption of the Second Payment Services Directive (PSD2), the Identity/Authentication roadmap has moved forward dramatically as one of the key cybercrime asset classes, and one of the most likely candidates for higher level eIDAS requirements.

COMPREHENSIVE LEGAL SYSTEM TO FIGHT AGAINST CC/CT

This topic reflects the current needs and challenges that facilitate requirements for improvements to the legal systems and related processes that impact upon all phases of cybercrime cases. One of the main efforts to be done in this area is the improvement of digital forensic products, services and procedures. In particular, it is important to ensure an adequate flow of information at the different stages of the investigation - from disclosure of crime, securing and preserving evidence and its processing, up to the judicial decision.

In this context it is also important to ensure and develop appropriate levels of knowledge and expertise across all the actors involved in the judicial process. The major improvement in information sharing and cooperation between victims, LEAs (the Police), the prosecution and forensic experts and finally the judges/courts is needed.

SUBMIT YOUR OWN IDEAS FOR FUTURE RESEARCH ITEMS AT

BIT.LY/CYBERROADMAP

COURAGE

CYBERCRIME and
CYBERTERRORISM
EUROPEAN RESEARCH
AGENDA

COURAGE PROFILE

CYBERCRIME AND CYBERTERRORISM EUROPEAN RESEARCH AGENDA

The COURAGE (Cybercrime and cyberterrOrism (E)UropeanResearch AGEnda) project is funded by the European Commission's seventh framework programme for research. COURAGE will produce a research agenda and roadmap for cybercrime and cyberterrorism using the expertise of the consortium partners, advisory board members and the project's extended network of domain experts and stakeholders.

The research agenda will identify the major challenges; reveal research gaps and recommend practical research approaches to address these gaps through strategies that are aligned to the real-world world requirements of practitioners, policy makers, citizens and other stakeholder groups. These strategies will be supported by test and evaluation schemes defining metrics and performance indicators used to assess the impact of actions taken as a result of the project's research roadmap. COURAGE's work is undertaken with the overall objective of defining practical, grounded approaches that will assist in supporting business and critical infrastructures, the capability of crime investigators and enhancing the overall security of European society as a whole.

To achieve this, COURAGE has undertaken to address a broad range of key challenges, such as the speed and implications of technological change, raising awareness and education levels, the transnational scope and nature of cybercrime, data protection and cooperation and information sharing issues, amongst others. The COURAGE approach is based on three pillars:

1. A user centric methodology - to identify gaps, challenges and barriers based on real-world needs and experiences.

2. An analytical and semantic approach - to deliver taxonomy; create a common understanding of the subject, and to review current and existing approaches and initiatives aiming to positively impact upon the domain.

3. A competitive and market oriented approach – to foster the practical implementation of counter-measures, using effective test and validation solutions.

https://www.courage-project.eu/

@FP7_COURAGE

COURAGE PARTNERS

European Organisation for Security

CENTRIC, Sheffield Hallam University

United Nations Interregional Crime and Justice Research Institute

Cybercrime Research Institute

TNO

Swedish Defence Research Agency

Office of the Police and Crime Commissioner for West Yorkshire

Engineering Ingegneria Informatica

Aconite Internet Solutions

EstEnter Polska

Conceptivity SARL

Institut Jozef Stefan

Selex ES SPA

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation

Tilburg University

International Cyber Investigation Training Academy

CAMINO
N
NE
E
SE
S
SW
NW

CAMINO PROFILE

COMPREHENSIVE APPROACH TO CYBER ROADMAP COORDINATION AND DEVELOPMENT

The CAMINO (Comprehensive Approach to cyber roadMap coordINation and develOpment) project was founded with the goal of providing a roadmap for improving resilience against cybercrime and cyber terrorism. The consortium has roots in the Integrated Mission Group Security (IMG-S) Cyber Theme Area, where the cyber security partners have an extensive experience in developing roadmaps. The participation of the Supporting Members in the CAMINO project, coming from Europe and North America (USA and Canada), ensured that the roadmap benefits from the vast knowledge and experience. The consortium have a very practical approach, with most partners being SMEs with a good understanding of what is realistic and practical and with an interest in finding a constructive roadmap complementing LEA and research organisations — without creating a bottleneck of problems and obstructions. The consortium used a holistic approach, analysing functions and capabilities addressing technical and human issues which are inter-related with legal and ethical aspects. We followed so called CAMINO THOR approach where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory. In each of the dimensions some items are proposed for the roadmap. In parallel with looking at the human and technical aspects, the project is focused on strong involvement of various different groups and operators such as LEAs, CERTS, personal users, governments, industry and research and commercial organisations. During the project we developed the CAMINO roadmap (research agenda). For each THOR dimension we identified 3-4 top priority topics that have to be addressed to more effectively fight against cyber crime and cyber terrorism. Each of these topics is described in the roadmap and is presented in the unified way. Topic description includes summary of key research objectives, summary of stakeholders with their roles in relation to given topic and detailed timeline. In this timeline we specified concrete milestones for three different time-spans (2017, 2020 and 2025). Such timelines briefly explain also current situation in given topic and expected (desired) end-vision at 2025, after the roadmap milestones achievement. Finally, topic timelines include summary of research activitiesthat should be performed, leading to the defined milestones achievement. Also, we constituted the CAMINO Cyber Think-Tank. Its main objective is the exchange of experience and knowledge, as well as the dissemination of information related to the effective measures against cyber crime and cyber terrorism. Its members would like to support national and international decision makers and EC in the area of cyber security.

http://www.fp7-camino.eu/

@fp7_camino

CAMINO PARTNERS

ITTI Sp. z o.o.

CBRNE Ltd.

Consiglio Nazionale delle Ricerche

Data Fusion Research Center AG

Espion Ltd.

Everis Aeroespacial y Defensa S.L.

Montpellier University

Police Academy in Szczytno

S21sec Information Security Labs S.L.

Sec-Control Finland Ltd

CYBER ROAD

CYBERROAD PROFILE

DEVELOPMENT OF THE CYBERCRIME AND CYBERTERRORISM RESEARCH ROADMAP

CyberROAD (Development of the Cybercrime and Cyberterrorism Research Roadmap) is a research project funded by the European Commission under the Seventh Framework Programme. The project is aimed to identify current and future issues in the fight against cybercrime and cyberterrorism in order to draw a strategic roadmap for cyber security research. The CyberROAD roadmap leverages on a sound roadmapping methodology and is built on top of a detailed snapshot of the technological, social, economic, political, and legal scenario on which cybercrime and cyberterrorism do develop. Within this scenario, research gaps and priorities are identified.

WHY CYBERROAD?

Recent studies on the evolution of the principal cyber threats reveal scenarios characterized by the growth of cyber criminal activities.

Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. The estimated annual cost over global cybercrime is 500 billion dollars (more than 500 million victims per year, 18 victims per second). More than 600000 Facebook accounts are compromised every day. In addition to the economic reasons, cyber attacks often hidden political and social motivations which constitute a serious threat to national security (hacktivism, cyber espionage, cyber warfare).

WHAT IS CYBERROAD DOING?

The main objective of CyberROAD is "developing the Cybercrime and Cyber-terrorism research roadmap". This roadmap is built through an in-depth analysis of all the technological, social, legal, ethical, political, and economic aspects on which cybercrime and cyber-terrorism are rooted. The research roadmap is being built by the means of a sound roadmapping methodology and by co-ordinating the efforts of the CyberROAD consortium along three key directions: Technology; Society; Cybercrime and cyberterrorism

The CyberROAD Consortium: The project, being implemented by a consortium of 20 partners from 11 different countries, relies on a large body of competences. The consortium, which is also supported by a board of external advisors, represents all the players and the stakeholders involved in the fight against cybercrime and cyberterrorism: law enforcement, public bodies, universities and research centers, as well as companies and industries.

https://www.cyberroad-project.eu/

@cyberroad_eu

CYBERROAD PARTNERS

University of Cagliari - PRA Lab

Technical University of Darmstadt - Germany

INDRA - Spain

Poste Italiane - Italy

SecurityMatters - Netherlands

Vitrociset - Italy

Foundation for Research and Technology - Hellas

INOV - Portugal

National Center for Scientific Research DzDemokritosdz - Greece

SBA Research - Austria

PROPRS Ltd - UK

Research and Academic Computer Network - Poland

Polícia Judiciária - Portugal

UINFC2

UINFC2 GET HANDS ON!

ENGAGING USERS AND PREVENTING AND FIGHTING CYBERCRIME AND CHILD SEXUAL EXPLOITATION

The vociferous proliferation of cybercrime has resulted not only in an increased number of reported incidents, but also in the ferocity, persistence, variety and potential impact (both societal and economic) of the underlying attacks on an increasingly diverse range of targets (i.e. persons, services, entities). This increase can be attributed to a range of factors, such as: a) the overall growth of the internet; b) the penetration of web services in our daily lives; as well as c) the latest technological achievements in ICT that enable many criminal actions to be transferred online; due to perceptions of anonymity and potential to obscure evidence. As one specific facet of this overall trend, the internet has seen a stark rise in its use as a vector for online sexual solicitation of children as well as the possession and subsequent distribution of explicit and abusive material.

In response, the UINFC2 project aims to assist in the cooperation and coordination among all major EU stakeholders, National Authorities, Law enforcement Agencies, National Hotlines & relevant EU bodies through the (real-time) provision of structured, analysed and correlated information. UINFC2's main objective is to design, develop and pilot a software platform providing intelligent analysis of collected or maintained data. The UINFC2 platform facilitates automated monitoring and inspection of provided data, as well as seamless crawling of suspicious content in the effort to identify the extent of possible incidents, information to make available to relevant stakeholders in order to enhance their capacity and capability to detect and remove explicit and abusive material from the web.

The platform will be tested during ongoing pilot operations carried out at a European level. The Input and feedback from these tests aims to capture end-user requirements and comments, leading to the refinement of the platform and the expansion of its functionality.

GET HANDS ON WITH THE PROJECT!

As part of this process, we're delighted to invite you to get hands on with the UINFC2 software platform over the course of the conference. You can find us situated in the conference staging area throughout the duration of the conference, so please feel to come and give the system a try for yourself!

http://www.uinfc2.eu/wp/en/

@UINFC2

European
Commission

These projects received funding from the European Commission's Seventh Framework Programme for research, technological development and demonstration under grant agreement numbers: 607306 (CAMINO), 607949 (COURAGE) and 607642 (CyberROAD) under FP7- SEC-2013.2.5-1.