Comprehensive Approach to cyber roadMap coordINation and develOpment

PROJECT FINAL REPORT

Grant Agreement number:	607406
Project acronym:	**CAMINO**
Project title:	Comprehensive Approach to cyber roadMap coordinatINation and develOpment
Funding Scheme:	Coordination and Support Action
Date of latest version of Annex I against which the assessment will be made:	2013-10-07
Periodic report:	**1st ■ 2nd ■**
Period covered:	from 2014-04-01 to 2016-03-31
Name, title and organisation of the scientific representative of the project's coordinator:	Prof. Michał Choraś ITTI Sp. z o.o. (Poland)
Telephone:	+48 600820317
Fax:	+48 616226973
E-mail:	michal.choras@itti.com.pl
Project website address:	http://www.fp7-camino.eu/

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement no 607406

Declaration by the scientific representative of the project co-ordinator

I, as scientific representative of the co-ordinator of this project and in line with the obligations as stated in Article II.2.3 of the Grant Agreement declare that:

- The attached periodic report represents an accurate description of the work carried out in this project for this reporting period;
- The project (tick as appropriate)[1]:
  - ■ has fully achieved its objectives and technical goals for the period;
  - □ has achieved most of its objectives and technical goals for the period with relatively minor deviations;
  - □ has failed to achieve critical objectives and/or is not at all on schedule.
- The public website, if applicable
  - ■ is up to date
  - □ is not up to date
- To my best knowledge, the financial statements which are being submitted as part of this report are in line with the actual work carried out and are consistent with the report on the resources used for the project and if applicable with the certificate on financial statement.
- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status.

Name of scientific representative of the Co-ordinator: Michał Choraś

Date: 30 / 05 / 2016

[1] If either of these boxes below is ticked, the report should reflect these and any remedial actions taken.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement no 607406

TABLE OF CONTENT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

1. EXECUTIVE SUMMARY

The CAMINO project was fully in line with the DoW and the planned schedule, and we achieved all the planned objectives and milestones without major problems and delays.

We completed and submitted 20 deliverables as planned. All of them were finalised without major delays. Also, all (seven) milestones have been met according to the predefined schedule.

All project success criteria were continuously monitored (please see Table 1 in section 2). The expected values of success indicators were achieved at the end of the project, and some of them are even **overachieved.**

The major result of the project is the comprehensive CAMINO Roadmap to fight against cybercrime and cyber terrorism. The proposed roadmap items were broadly consulted with end-users and experts and then validated and prioritised at consultations, meetings and validation exercises.

Also, we organised more (seven) CAMINO workshops than initially planned in the DoW (where we stated that four CAMINO events will took place).

Moreover, we have achieved a wide dissemination of the project, exceeding expected number of participants present to the workshops (we had more experts participating in the workshops than the number we promised to invite), conference presentations, and website visitors.

One of the most important activities done during the project was community building. Establishing the CAMINO Cyber Think Tank will allow us to follow the comprehensive approach and to keep alive our Roadmap after the project, assuring sustainability of the CAMINO concepts and ideas. Moreover, we had a very fruitful collaboration with other CSA projects, namely COURAGE and CyberROAD.

The goal of this report is to summarize achievements and results of 24 month collaborative work. In Section 2 we present the main objectives (general and detailed) and the overall context of project. Section 3 describes results of the project: analysis of cyber crime / cyber terrorism threats, our workshops and finally most important project products: the CAMINO roadmap and the practical guidelines. In Section 4 considerations on the project potential impact are provided.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

2. SUMMARY DESCRIPTION OF PROJECT CONTEXT AND OBJECTIVES

The ever-increasing adoption of computing technologies and online access has led to significant economic and societal gains, yet such benefits are jeopardised by threats, both real and imagined, to the security of the underlying technology and in how it is currently deployed. While legitimate businesses and public organisations leverage new ICT technologies in positive ways, growing numbers of opportunistic and organised criminals seek to take disparate advantage, motivated along different lines ranging from economic profit motives, to ideological activism or terrorism.

The main goal of the CAMINO project was to establish a research agenda on cybercrime and cyber terrorism in order to fully accomplish a trustworthy information society as depicted by the Digital Agenda 2020.

We identified two main strategic objectives:

Main Strategic Objective 1: to develop a comprehensive cybercrime and cyber terrorism research agenda,

Main Strategic Objective 2: to initiate long term activities providing a stable platform of security research experts and organisations.

In addition we defined the following 6 Detailed Objectives:

Detailed Objective 1: to define a concept and terminology of cyber security, cyber crime and cyber terrorism. This CAMINO objective will unify and describe cyber-related terminology and to achieve common understanding of major concepts within the community. One of the means to achieve this goal will be via meetings, workshops and engagement with expert panels.

Detailed Objective 2: to identify current cyber threats (including cyber crime and cyber terrorism) and corresponding state-of-the-art identification, protection and defence mechanisms, including appropriate risk analysis methodologies. This objective will identify and describe current and future- cyber threats, including cyber-crime and cyber-terrorism risks of various organisations and stakeholders such as CERTs, industry, private companies, public administration, critical infrastructures, SMEs, and individual users among others. One approach towards this goal will be a set of meetings, workshops and talks to experts (e.g. via the CAMINO expert panel). We will also discuss these aspects with CAMINO supporting members, allowing spectrum broad discussion of threats and risks.

Detailed Objective 3: to define research gaps and stakeholders needs. This objective will identify, and define major research gaps and stakeholder needs (via workshops, questionnaires, via engagement with Supporting Members and expert panels, etc.). We will define multidimensional needs using our THOR (Technical and testing capabilities, Human, Organisational and Regulatory) approach. The identified gaps, requirements and needs will drive research agenda development activities.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Detailed Objective 4: to propose and publish guidelines, recommendations and a comprehensive research agenda (roadmap) regarding cyber security, cyber-crime and cyber-terrorism. This objective will provide a comprehensive roadmap, also using the aforementioned THOR (Technical and testing capabilities, Human, Organisational and Regulatory) approach. The roadmap will contain short-, mid-, long- term research agendas across all of these dimensions. Guidelines and recommendations will be provided to complement the research agenda (CAMINO roadmap), along with proposed solutions and means to solve current cyber-crime and cyber-terrorism gaps. Such roadmap and guidelines will address needs of various stakeholders such as CERTs, public administration, law enforcement agencies, utilities, industry, individual users, etc., since SME-based consortium has daily access to those actors.

Detailed Objective 5: to build a long term cyber research community on the basis of the IMG-S Cyber Security Thematic Area (TA7). While developing CAMINO roadmap and guidelines, the long-term research community will be established. The basis of such experts and stakeholders group is the IMG-S Cyber Security Thematic Area. However, thanks to huge dissemination potential and community relations of this group, we managed to reach out effectively to the wider community even at this early proposal stage. We also have a support of 21 Supporting Members. Dedicated tasks for community building and cyber think tank creation are planned in WP5.

Detailed Objective 6: to provide dissemination and exploitation of the project results. This objective will effectively inform relevant stakeholders about the CAMINO project, the roadmap development process, and CAMINO workshops. This will support greater involvement of a wide spectrum of actors towards identifying gaps, threats, market status and opportunities, related risks and stakeholder needs. We will also disseminate our community building efforts and progress. Dissemination is also needed for wide roadmap consensus and adoption. Once the roadmap is developed we will actively disseminate it in the relevant communities. We also plan CAMINO presence at relevant events and a strong presence in electronic media (web-based).

These overall objectives are broken down into detailed project objectives for each of the work packages and were continuously monitored and evaluated by taking into account measures (success criteria) defined at the early stage of the CAMINO proposal. The final (at M24) status of the CAMINO success criteria is presented in Table1.

Table 1: CAMINO success criteria - final status.

Measure	Description	Related WP	Expected number	Current number	Status
Contact with Expert Panel	Experts interviewed and surveyed	WP2	25	>30	achieved
Stakeholders identification	Stakeholders identified	WP3	50	>100	overachieved
Workshops, consultations	Workshops executed	WP3 WP5	4	7	overachieved

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

	Participants invited		100	>2000	overachieved
Guidelines	**Guidelines developed**	**WP4**	**1**	**1**	**achieved**
Roadmap	**Roadmaps developed**		**1**	**2**	**overachieved** (including consolidated roadmap prepared in cooperation with COURAGE and CyberROAD projects)
Research community	Organisations contacted	WP5	30	>100	overachieved
	Organisations building research communities and cyber think tank		15	>25	overachieved
Dissemination	Publications submitted and published		6	10	overachieved
	Conference presentations		6	>20	overachieved
Online presence	Project website popularity (number of visitors)		1000	>8000	overachieved
	Social media channels used to share project progress and results		3	3	achieved

3. DESCRIPTION OF THE MAIN S&T RESULTS/FOREGROUNDS

3.1 Summary of the project achievements

During two years of the project, the CAMINO consortium has fulfilled all detailed objectives defined for the particular work packages and tasks and has achieved all relevant milestones, set for the project.

More specifically, CAMINO consortium:

- **Delivered the final version of the CAMINO Roadmap (research agenda) – D4.4 deliverable,** with its adoption plan including identified and defined future steps ensuring effective dissemination and adoption of the CAMINO roadmap across the cyber security community,

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- Achieved all specific goals related to the WP2: Identification and Analysis of Main Research Gaps and Challenges, namely analyses of current cyber security efforts, cyber crime & terrorism related risk and market, current trends in cyber security, maturity level of technologies related to the fight against cyber crime, as well as identification of current research gaps, challenges and needs. Moreover, as a part of this WP we performed a number of interviews with members of our expert panel. WP2 has ended in the first year of the project and has provided a valuable input for the other project tasks, mainly related to the development of research agenda.
- Delivered the final CAMINO practical guidelines for fighting against cybercrime and cyber terrorism (D4.2),
- Organised and conducted all the planned expert workshops scheduled in the DoW:
    - 1st CAMINO Workshop on "Cyber Security and Physical Security" (18 September 2014, Bern, Switzerland) focusing on the present status of the fight against cyber crime and cyber terrorism and on end-user perspective,
    - 2nd CAMINO Workshop on "Mobile, Mobility and Cyber Security: How can IoT secured against cyber attacks?" organised during Mobile World Congress (3 March 2015, Barcelona, Spain),
    - Joint CAMINO/COURAGE Workshop (CAMINO/COURAGE cyber crime and cyber terrorism research agenda workshop) organised jointly with FP7 COURAGE project (8-9 April 2015, Montpellier, France). This workshop was devoted to presenting and validating the initial versions of the CAMINO roadmap and guidelines.
    - CAMINO Workshop in London on "Parameters for Guidance & Roadmap for the Prosecution of Cybercrime in Civil, Criminal & Common Law" (15-16 June 2015),
    - CAMINO Workshop for Supporting Members and Think-Tank Participants in Warsaw (19 January 2016),
    - CAMINO Final Workshop: "Cybercrime and Cyberterrorism Research Summit" in San Sebastián (3 March 2016),
    - COURAGE / CAMINO / CyberROAD Joint Workshop on "Emerging and Current Challenges in Cybercrime and Cyberterrorism" in The Hague (10-11 March 2016).
- Performed a large number of dissemination actions, including on-line presence of the CAMINO (social media, webpage), CAMINO presence at various scientific conferences and other events focused on cyber crime and cyber terrorism problems, submission of papers disseminating project's results:
    - Maintenance of the CAMINO website (www.fp7-camino.eu) and continuously updating it with the project news, relevant material (initial and final roadmap available), information about CAMINO workshops, including registration/accommodation advices, etc.,
    - Maintenance of and dissemination of project results and news through social media channels (e.g. Twitter, LinkedIn),
    - Development and printing of dissemination material, namely flyers, "roll-up", different versions of the final CAMINO Roadmap for the further use, etc.,

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- Preparing 7 scientific publications related to CAMINO,
- Presentation of the CAMINO at over 20 dissemination events (cybercrime/cyber security related conferences, workshops, seminars), including promotion of the CAMINO at the joint CAMINO-COURAGE-CyberROAD events,

- Performed a number of community building activities, such as cooperation with other CSA consortia, cooperation with CAMINO Supporting Members and finally built a strong and sustainable community (CAMINO Cyber Think-Tank established with 25 members from 10 different EU countries),
- Cooperated with FP7 COURAGE and CyberROAD project in order to prepare the consolidated roadmap.

3.2 Identification of main research gaps and challenges and analysis of cyber threat landscape

The initial work in WP2 work package was focused on the analysis of current cyber security, cyber crime and cyber terrorism guidelines, roadmaps, national strategies and relevant ongoing projects. We studied and summarised the broad range of background material, including sectoral roadmaps, general roadmaps, national strategies and ongoing projects with relevance to CAMINO.

In D2.1 report, we presented results of this analysis. We also presented the view of the Law Enforcement Agencies (the Police in particular) on current and future cyber crime and cyber terrorism problems, as well as results of the analysis of the current legal regulations, conventions and directives regarding cyber crime and cyber terrorism. The output of this document, is the broad view on current roadmaps and initiatives, but more importantly on current cyber security, cyber crime and cyber terrorism countering technologies challenges, gaps, improvements and research needs (according to the authors of roadmaps and strategies and based on project goals). It is worth mentioning, that our goal was not to compare or judge those background documents, but to focus on the analysis in the context of CAMINO.

This task addressed the initial set of problems and research requirements (or at least took them into account) for the development of the CAMINO roadmap. Of course, this analysis was only the first step and has been revised during the CAMINO workshops, consultations, dialogue with the relevant stakeholders. In particular, aspects emphasised in D2.1, include:

- Evaluation of system security,
- Identity management mechanisms,
- Growing problem of malware and botnets,
- Improvements of analytical tools for security monitoring, response and recovery efforts and security-related information analysis,
- Privacy-related problems,
- Situational understanding.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The main recommendation for the CAMINO roadmap was diagnosis that the most serious threats for existing and future cyber systems are malware, botnets, as well as identity- and privacy-related threats. The most promising measures for countering such cyber crimes are investments in systems security evaluation, improvements of analytic capabilities and information/knowledge sharing.

The main output of Task 2.2 was D2.2 deliverable. This deliverable is divided in 6 main parts presenting the results of the risk and market analysis performed by the consortium members. This analysis is focused in the identification of:

- Assets to protect,
- Assets' vulnerabilities,
- Main threats and possible attacks,
- Threat agents and motivations for the launching of a cyber attack,
- Risk facing the assets,
- Future Trends regarding threats.

Moreover, the document includes a chapter related with the solutions needed to at least mitigate the impact that the threats may generate, and although the countermeasures will be the main content of the roadmap to define, definition and some general aspects to consider are reviewed.

We based on the Magerit risk assessment methodology to achieve the main goal of the deliverable - the identification and quantification of the risks of possible cyber attacks over the selected assets. Our approach enabled research to quantify the value of the selected assets, the risk facing those assets and then defining the measures needed for their protection.

Considering the results of our risk analysis, the assets with the highest average risk are payment systems, embedded systems, banking & financial services, personal data, cloud infrastructures, and intellectual property rights. Those assets make up the top 6 of the assets, over which there is a bigger risk, considering the risk as the level or probability that the asset is affected by the threats identified.

Reviewing the results, they are very coherent due to the current main target of cyber crime, very focused with all the processes related with digital payment systems where banking and financial services can also be included. And regarding the other assets in the top 6, it found the embedded systems, being part of bigger systems in many different fields can be threatened due their own design process. Following which, both Personal Data and Intellectual property information are also a target for illegal activities related mainly with cyber crime, so the risk to which they are exposed is quite high.

This classification does not mean that the CAMINO roadmap focuses solely on launching actions to protect these top 6 groups of assets, as there are other variables to take into account.
The D2.3 report (Current Trends and Maturity Level) is the document describing output of T2.3 analyses, focuses on the following aspects:

- How the technology inventory was scoped,

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- Scoring system for evaluation of each technology,
- How to use the inventory,
- Analysis on trends and challenges of each technology.

In the background of this activity, we also created the additional spreadsheet file (.xlsx) with the assessments.

We have analysed over 40 different technologies and over 110 sub-technologies. According to our analysis 83,3% of them are of high readiness level (7-9). Only 8,3% are identified as being of medium (4-6) and low readiness level (1-3). All the analysed technologies have been identified as those being capable of providing reactive mechanisms. Over 87% and 64% have been identified as proactive and real-time respectively. In the report, it is also shown how different technologies are distributed among TRL and Gartner Hype Cycle Levels. It can be noticed that 54,2% of the analysed technologies have been identified as those having high both TRL and Gartner Hype Cycle levels. The implication of this could be the fact that those technologies are less likely to be further researched and evolved. Therefore, the recommendation to be considered in the roadmap, is focusing on remaining 10,4% of technologies having low and medium TRL as well as GHC lower than 5.

Concluding, the provided analysis served as important background for further CAMINO roadmap development process. First of all, the further work could put the emphasis on emerging and less mature technologies that are likely to become widely accepted in the near future. Among those technologies we indicated:

- Cyber fraud prevention technologies,
- Denial of Service (DoS) / Distributed Denial of Service (DDoS) Protection,
- Internet of Things (IoT) Security,
- Intrusion Detection Systems,
- Advanced Persistent Threat (APT) Detection,
- Cloud Forensics,
- Cryptography,
- Technical Security Standards,
- Big Data Security Analytics,
- Cloud Security.

The second recommendation for the roadmap was that we must focus on technologies that provide all types of the identified capabilities, namely: proactive, reactive, and real time.

Goal of T2.4 task was to identify main concerns regarding cyber crime and cyber terrorism, e.g. the main assets to protect, threats, protection technologies etc. Moreover, human and ethical aspects are also addressed. The consortium used two means to realise the task:

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- The questionnaire consisting of 13 questions regarding cyber crime, cyber terrorism and cyber security aspects such as:
    - Assets to be protected and its criticality evolution due to a potential impact,
    - Main threats to face when protecting the assets,
    - Better methods to fight against the threats, by technological means, regulations, etc.,
    - Most common vulnerabilities and how they are evolving,
    - Impact arising from a cyber attack by the identified threats and it possible evolution,
    - Most required cyber security technologies in short and long terms,
    - Top 5 of disruptive technologies,
    - Main cyber attacks agents and the most frequent illegal activities,
    - Principal human and ethical issues regarding cyber security aspects.

- Interviews (face to face, telephone), following the previously commented topics and others challenges and trends faced by the responders.

Up to 30 experts answered the questionnaire - all of them covering different roles and responsibilities as:

- Engineers
- Researchers
- Managers
- Security Experts
- Senior Consultants
- CEOs

Consortium members also interviewed a total number of 25 experts.

After reviewing the results collected from the survey and also considering main challenges and trends from the face-to-face interviews, the main conclusions and challenges to be considered can be summarised like follows:

- Attacks on Critical Infrastructures have potentially bigger impact to the society, however, their risk to be attacked is rather low.
- Main threats are those with a concrete target to achieve and with more resources, e.g., state-sponsored attacks, it should be noted the APTs include many different attack vectors, and also the denial of service attacks (DoS) to stop the operating of important systems.
- It is critical to launch actions to increase the cyber security awareness and culture of the citizens and also improve the training for those fighting against cybercrime and cyber terrorism.
- The implementation of security aspects from the design phases of every new systems or application should be regulated.
- It is critical for the European companies to implement technologies and measures protecting them from intellectual property theft.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- It is necessary to invest and focus the technological development in those technologies offering intelligence to the security responsible, changing the reactive methods for other proactive ones making possible to act in advance of a cyber attack.
- It is necessary to adapt laws and regulations to address the special characteristics of cyberspace in order to facilitate the work of the LEAs and not to facilitate the work of the "bad guys". Creating a multi-domain source of information including the exchange of expertise between stakeholders.
- To boost information exchange methods and cooperation between international police forces and also between the public and private sector to help in the cybercrime fight.
- In order to consider the special characteristics of the CLOUD services, it is necessary to adapt the laws and regulations under which the CLOUD services providers should be regulated.

In task T2.5 the comprehensive THOR (Technical, Human, Organisational, Regulatory) analysis of the current gaps and challenges of possible means to counter cyber crime and cyber terrorism was performed.

Following the THOR approach, the D2.5 document encompassed challenges to face, capabilities to improve or actions to launch in order to address a better overall situation when trying to fight against cyber crime and cyber terrorism actions.

In Table 2 the identified aspects divided in THOR dimensions are presented.

Table 2 Gaps and challenges identified in this document

THOR dimension	Identified gaps and challenges
T	• Fight against growing and evolving malware and botnets • Denial of Service (DoS)/Distributed Denial of Service (DDoS) protection • Intrusion Detection Systems • Big data for cyber security analytics • Cloud Security and cloud forensics • Internet od Things (IoT) • Information sharing platforms and mechanisms • Authentication and Authorisation • Mobile devices protection • Protection from APTs (Advanced Persistent Threats) • Insider threats detection and protection • Testing capabilities

H	• Training, awareness and management/monitoring/mitigation with respect to:
	  ○ Consumers
	  ○ Judiciary
	  ○ LEAs
	  ○ Organisations
	• Ethical dimension of corporate/nation state reaction to cyber crime/-terrorism events

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

	• Psychological contract • Privacy and security in its wider socioeconomic context • Ethically responsible cyber security research • Individual rights vs. societal rights; lawful interception, including intra-jurisdictional 'illegal' lawful interception; protecting Individual privacy in the struggle against terrorists
O	• The challenge of the global nature of the Internet • Good practice in security self-defence is an issue of culture and commitment in the organisation • Generic challenges due to the nature of cyber crime • Generic challenges and obstacles at the enterprise/company/SME level
R	• Lack of common regulations and differences in legal systems • Technical language and cyber definitions in law • Slow evolution of law • Regulations and standardisation for anonymity and privacy on the Web • Regulations for trans-border cyber crimes/terrorism, investigations and data gathering • Regulations on new forms of data processing and analysis (BD, IoT) and cyber crime

After performing the analysis presented in this deliverable and also taking into account all the findings and data collected from the previous work in WP2, it was clear that the required solution facing the new cyberspace threats, cyber crime and cyber terrorism, should not be focused only on one particular area, but a holistic approach is needed (such as CAMINO THOR).

Technology without laws and regulations that allow the carrying out of special measures would not be successful, and on the other hand, an evolution in the regulations without the technological ability to execute or to defend those regulations would have no meaning at all.

3.3 CAMINO workshops

In WP3 and WP5 we organized 7 workshops for the project end-users and cyber security experts. The main conclusion is that the CAMINO consortium had the clear vision of the workshops' organisation, differentiation of the workshops for the various targeted group of experts and the expected impact on the further project's course.
The short characteristics and facts related to each workshop conducted during the project are presented in next sub-sections.

3.3.1 1st CAMINO Workshop in Bern

The first workshop took part in Bern (18 September 2014) in Kursaal.

The Consortium (the organisation was led by DFRC) invited about 750 experts and 58 of them registered to the workshop. The attendance was 58 participants.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The workshop consisted of CAMINO presentations, invited keynote speakers (mainly industrial) and time planned for networking and community building (lunch, coffee, etc.).

We consider the workshop as a great success, while the lessons learnt were analysed the next day at the consortium meeting and will be used to improve the next CAMINO events.

The agenda and the presentations are available at: http://www.dfrc.ch/camino-workshop.

3.3.2 2nd CAMINO Workshop in Barcelona

The second workshop took part in Barcelona (3 March 2015), during the Mobile World Congress days.

The goal of the event was to gather experts in Internet of Things, Big Data and mobile and foster the exchange of research, solutions and opinions, with a common focus on the Cyber Security threat.

The Consortium (the organisation was led by DFRC) invited 948 experts and 231 of them registered to the workshop. The attendance was 122 participants.

11 talks presented the state-of-the-art solutions to Cyber Security threats. Experts tried to answer the following questions: Which are the scenarios at risk? Which procedures and methods for Security Assurance? How do Automated Intrusion Response systems work? How do we guarantee end-to-end security for IoT and cloud services? Where are researchers and companies going to protect cellular communications and transport management systems from hackers?

During the workshop another FP7 CSA CyberROAD was also presented.

Last but not least, the workshop presented the opportunities for SMEs in the Cyber Security industry and the support of the European Union in addressing these needs, not only in terms of business benefits but as value for all citizens.

We consider the workshop as the significant success, based on the very interesting content presented by international experts and high number of attendees.

The agenda and the presentations are available at http://www.dfrc.ch/event/mobile-mobility-cyber-security/. All the videos are available on https://www.youtube.com/user/DFRCch

3.3.3 Joint CAMINO/COURAGE Workshop – Montpellier

This workshop entitled “Innovation and Cybercrime: Challenges of the digital transformation in Europe” was held at Montpellier University (8 and 9 April 2015).

This event was the first CAMINO workshop organised jointly with other Cyber Security CSA, COURAGE, and so is the result of the process of reflections and exchanges promoting the vision of the European cyber security and to reinforce the struggle against cyber criminality, priority of the European Union for which both projects were elaborated.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Taking the opportunity of the fact the workshop was a part of two-days Montpellier Congress and took place in University of Montpellier, the main objectives were:

- to present the first versions of CAMINO Roadmap and Guidelines to research community and to receive their opinion and feedback,
- to provide SMEs, industry sector, scientific communities and end users, a forum to exchange visions and challenges addressed by CAMINO and COURAGE projects.
- to offer a forum to reflect on the development of strategies to achieve these goals

The parallel objective, from the point of view of CAMINO consortium, was to explore complementarities with COURAGE project and also possibilities of closer cooperation.

Particularly, the scope of the conference was to gather the ideas regarding cyber security in Europe and beyond, and to discuss the methodology's progress, the technology and the foundations for the conception and the effective display of cyber security, which grant the realisation of the guidelines and the recommendations to the European commission and to citizens.

Two days of the workshop were planned around 5 sessions presided and animated each by personalities and cyber security experts (European institutions and organisations, academic sector):

- Analysis of risks and strategies regarding cybernetics threat
- Aims and risks related to the development of bit coins
- Big data, Internet gadget, and security
- European projects, international cooperation, research and formation in the field of the struggle against Cyber criminality and Cyber-terrorism
- Presentations of the first outcome of CAMINO and COURAGE's projects

143 participants have registered to the conference, and 126 were present.

3.3.4 3rd CAMINO Workshop – London

The workshop entitled "Parameters for Guidance & Roadmap for the Prosecution of Cybercrime in Civil, Criminal & Common Law" took part in London (15 and 16 June 2015), at Royal Holloway University.

The objective was to gather together experts in criminal and common law and foster the exchange of research, solutions and opinions regarding the prevention and prosecution of cybercrime.

The difficulties in measuring cybercrime were outlined, in particular the problem of being able to report crime, let alone finding an LEA able or willing to investigate it. The disparity of the regulatory approaches in different countries increases the difficulty of understanding the scale of the problem.

The Workshop discussed the forthcoming harmonisation through EU Regulations, in particular the impact that would be felt as a result of the Data Protection and Electronic Identity, Authentication and

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Signatures (eIDAS) regulations. Changes are imminent to the legal definitions of privacy, the necessary levels of assurance and the new requirements for strong authentication.

The need for standards was discussed based on getting a better understanding, not only of the scale of the issues, but also what the stakeholders expect and when. A second consistent theme was the willingness of stakeholders to come together to help understand their roles. The need for wider appreciation of the nature of cyber regulations was readily apparent from the lively industry questions about the relevance of data protection regulations to industry standards, with some delegates unaware of the all-encompassing controls soon to be introduced.

The workshop agreed important aspects to be integrated into the CAMINO roadmap as follows:

- Cyber insurance (which was a very important topic raised many times by the experts during the two days) as well as incentives towards cyber insurance
- Data breach notification regulations, incentives and lessons learnt,
- Improving information sharing, also reporting on attacks not only successful intrusions
- Better communication to consumers/citizens (which is already addressed, but will be emphasised in our roadmap)
- Focusing on awareness and teaching
- Building on success stories and successful cases
- Creating standard rules of engagement (e.g. for LEA)

The workshop closed with final remarks by Professor Choraś inviting delegates to the interim fourth workshop in San Sebastian in March 2016. The workshop at Royal Holloway will catalyse the promulgation of the CAMINO, roadmap and guidelines alongside sibling programmes CyberROAD and COURAGE.

101 attendees registered to the workshop. On the first day, there were 78 attendees, including 15 panel members and keynote speakers, on the second day, there were 42 attendees, including nine panel members and keynote speakers.

3.3.5 CAMINO Workshop for Supporting Members and Think-Tank Participants – Warsaw

The workshop was organised for the CAMINO Supporting Members and members of the CAMINO cyber Think-Tank in Warsaw (19 January 2016) at *Krajowy Punkt Kontaktowy Programów Badawczych Unii Europejskiej* (Polish NCP). The main objective of this event was to present, discuss and validate the pre-final version of the CAMINO roadmap (D4.4) 2 months before its finalisation. The feedback from cyber security experts and practitioners was expected to be a valuable input to the roadmap development and final changes/improvements.

The validation exercise and comments by experts gave valuable feedback to the final roadmap. The results of the validation are presented in D4.4 CAMINO Roadmap.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

3.3.6 CAMINO Final Workshop – San Sebastián

The Final Workshop of CAMINO Project entitled "Cybercrime and Cyberterrorism Research Summit" was organised by S21sec in collaboration with ITTI, DFRC and CBRNE in San Sebastian (3 March 2016). It was held in the last month of the project, aiming at presenting the main results, roadmap, and guidelines, together with other blocks that summarises the overall thinking of the project in the fight against cybercrime and cyber terrorism.

The audience of this workshop was from diverse communities and domains. Law Enforcement Agencies, companies, universities and public bodies registered to attend the workshop, which was a very valuable asset. The workshop was attended by 98 experts.

This workshop is the final one, where the main results and topics discussed during the project lifetime were presented. The aim of the workshop was also to cover different topics related to the fight against cybercrime and cyber terrorism.

Professor Michał Choraś made a final presentation that covered these main results, encouraging attendees to give us the final feedback through a questionnaire.

The workshop closed with final remarks by Professor Choraś inviting attendees to the COURAGE – CAMINO – CyberROAD joint conference in The Hague on 10-11 March 2016.

More detailed information related to the event in San Sebastián was reported in the deliverable D5.3.

3.3.7 COURAGE /CAMINO / CyberROAD Joint Workshop – The Hague

The event was held in the Hague (10-11 March 2016, International Press Centre Nieuwspoort) and was part of an overall thinking and exchange process that aims at promoting a European vision and roadmap for the fight against cybercrime and cyber terrorism, a priority for the European Union and the basis upon which all three projects were initiated. Over 90 participants registered to attend, and over 60 attended the event.

The objective of the joint workshop was to provide SMEs, the industry sector, scientific communities and end-users a forum to exchange ideas and challenges presented by the projects in order to elaborate strategies and priorities for a common roadmap to fight cybercrime and cyber terrorism.

In particular, the goal of the two-day event was to gather insights regarding cybercrime and cyber terrorism in Europe and beyond, and 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 cyber terrorism.

The consolidated, joint CAMINO - COURAGE - CyberROAD research agenda was validated by the experts who attended this Workshop.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The first version of the consolidated roadmap was validated. This roadmap included topics by CAMINO and COURAGE (yet without CyberROAD). Of course, CAMINO roadmap was also presented and discussed. The outcome is also the discussions on the current problems and new ideas to counter them (e.g. expressed during presentations by the Police (Poland, UK) and EUROPOL).

3.3.8 Seminar co-organised by WSPol

In addition to the described five CAMINO workshops, one of the CAMINO partners – WSPol co-organized event entitled "Countering and fighting cybercrime" (*pol. Przeciwdziałanie I zwalczanie cyberprzestępczości)* held in Warsaw, 31st March 2016. This was the 'invitation-only' event (not open), mainly for LEA and experts in security and military aspects. Organisers gathered over 110 participants, also from abroad (the US, UK and Romania) including broad spectrum of experts from academia, LEA, courts, banks and prosecutor's office. One of the main aspects discussed was need for the comprehensive system to fight cybercrime – as suggested by CAMINO and proposed in our Roadmap and included also in the consolidated roadmap.

3.4 CAMINO products - comprehensive roadmap and practical guidelines

D4.4 document - CAMINO roadmap (research agenda) - was delivered in M24. This document is the final version of the CAMINO research agenda (roadmap) to fight against cybercrime and cyber terrorism. The initial (preliminary) roadmap was drafted in March 2015 and was reported as D4.3.

This roadmap (research agenda) is the most crucial product of the 2-year project. It answers the question 'where the money should be invested to counter cybercrime and cyber terrorism?' It also gives advice on which research topics are important in order to increase cyber security and resilience with respect to cybercrimes.

The proposed roadmap items were broadly consulted with end-users and experts and then validated and prioritised at consultations, meetings and validation exercises.

Our approach for the CAMINO roadmap development is based on the THOR concept. THOR dimensions are the foundation of the CAMINO roadmap scope and structure.

THOR dimensions address the following aspects:

- (T)echnical – related to technology, concrete technological approaches and solutions that can be used to fight against cybercrime and cyber terrorism,
- (H)uman – related to human factors, behavioural aspects, privacy issues, as well as raising awareness and knowledge of society with regards to cybercrime and terrorism threats,
- (O)rganisational – related to processes, procedures and policies within organisations, as well as cooperation (public-private, public-public) between organisations,
- (R)egulatory – related to law provisioning, standardisation and forensics.

The roadmap is focused on these four key pillars of cyber security research, presenting the main objectives, problems, challenges and associated stakeholders from each dimension.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

We divided each of THOR dimensions into several (3-4) topics – areas of interest. These topics are based on Consortium expertise, previous WP2 gaps analysis and opinions of the stakeholders and experts. All these inputs provide a view on common gaps and challenges that need to be overcome in the fight against cybercrime and cyber terrorism. Summary of dependencies between WP2/WP3 and our roadmap is depicted in Figure 1.

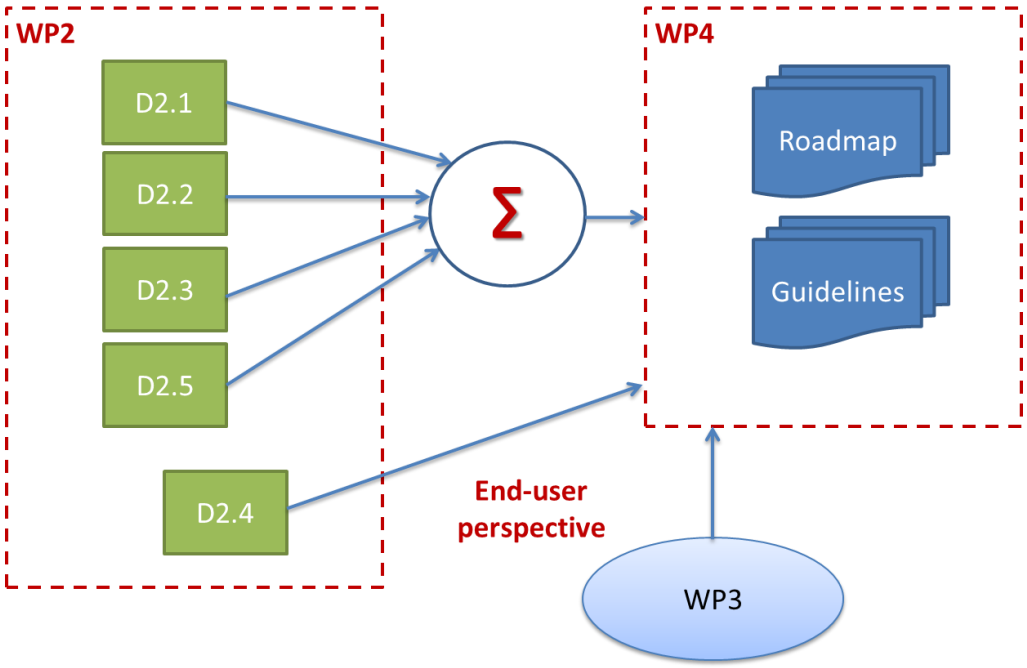

Figure 1: CAMINO roadmap dependencies and inputs

The CAMINO roadmap structure with dependencies between THOR dimensions, topics, objectives, milestones and actions is presented in the Figure 2.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

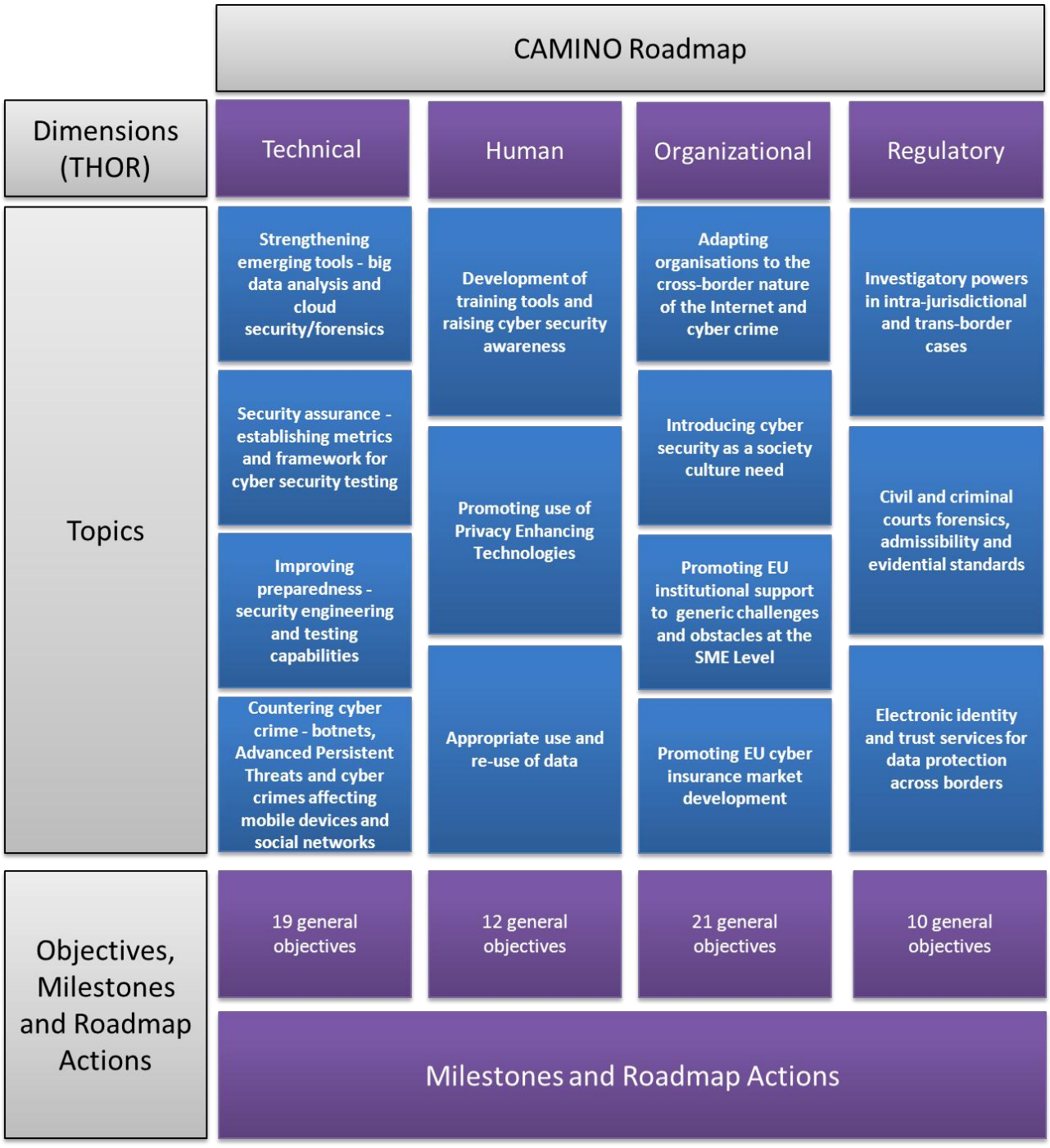

Figure 2: CAMINO roadmap structure

Each topic addressed in our roadmap is described in dedicated sub-section and is presented in a unified way, including:

- Summary of key research objectives related to a given topic.
- Summary of stakeholders with their roles and who should participate in the specific research subject.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- Detailed timeline for concrete milestones and specified for three different time-spans (2017, 2020 and 2025). Such timelines briefly explain the current situation in a given topic and the expected (desired) end-vision at 2025, after the roadmap milestones achievement.
- Summary of research activities that should be performed leading to the defined milestones achieved.

Topics from the Technical Dimension are focused on big data and forensic aspects, improvement for authentication and authorisation mechanisms, security engineering and testing capabilities, as well as means for an effective fight against malware, botnets and APTs (Advanced Persistent Threats). The Human Dimension emphasises the need for mechanisms regulating the use and reuse of personal data and training and raising cyber security awareness. Topics from the Organisational Dimension part of the roadmap are focused on societal and cultural aspects of cyber security, on adaptation of the organisations in light of the international nature of cybercrime and cyber terrorism, as well as on cooperation between organisations (e.g. SMEs) and supporting EU institutions. The development of the cyber insurance market is also one of topics in the Organisational Dimension. Finally, the Regulatory Dimension is composed of aspects of investigatory powers, forensics and standards of evidence and data protection across borders.

For each topic, the roadmap specifies a number of objectives with assigned milestones and actions to achieve those milestones. In total, the Project has identified over 60 objectives and over 250 milestones considered as micro-steps in our research agenda, leading to a more effective fight against cybercrime and cyber terrorism up to 2025.

In comparison to the first (initial) version of the CAMINO roadmap (drafted in March 2015 and reported as deliverable D4.3) we specified some existing points in the research agenda and added new ones to make the CAMINO roadmap more comprehensive during the second year of the CAMINO project. Some of the changes have been applied in accordance with the validation results. The main changes done in this period (after M12) were as follows:

- Changed names of the research agenda topics,
- Updated objectives, milestones and actions in selected topics,
- Changed timeline for selected actions, e.g. some of actions have been shifted from long-term (10 years) to mid-term (5 year) perspective, etc.,
- Added “Promoting EU cyber insurance market development” topic in the Organisational Dimension as our answer to the London Workshop feedback, where cyber insurance aspects were widely discussed,
- Merged two regulatory topics: "Interoperability of Common and Roman Law" with "Investigatory powers in intra-jurisdictional and trans-border case" into one topic.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The summary of roadmap activities for each THOR dimension and timeline (short-medium-long) is presented in next figures.

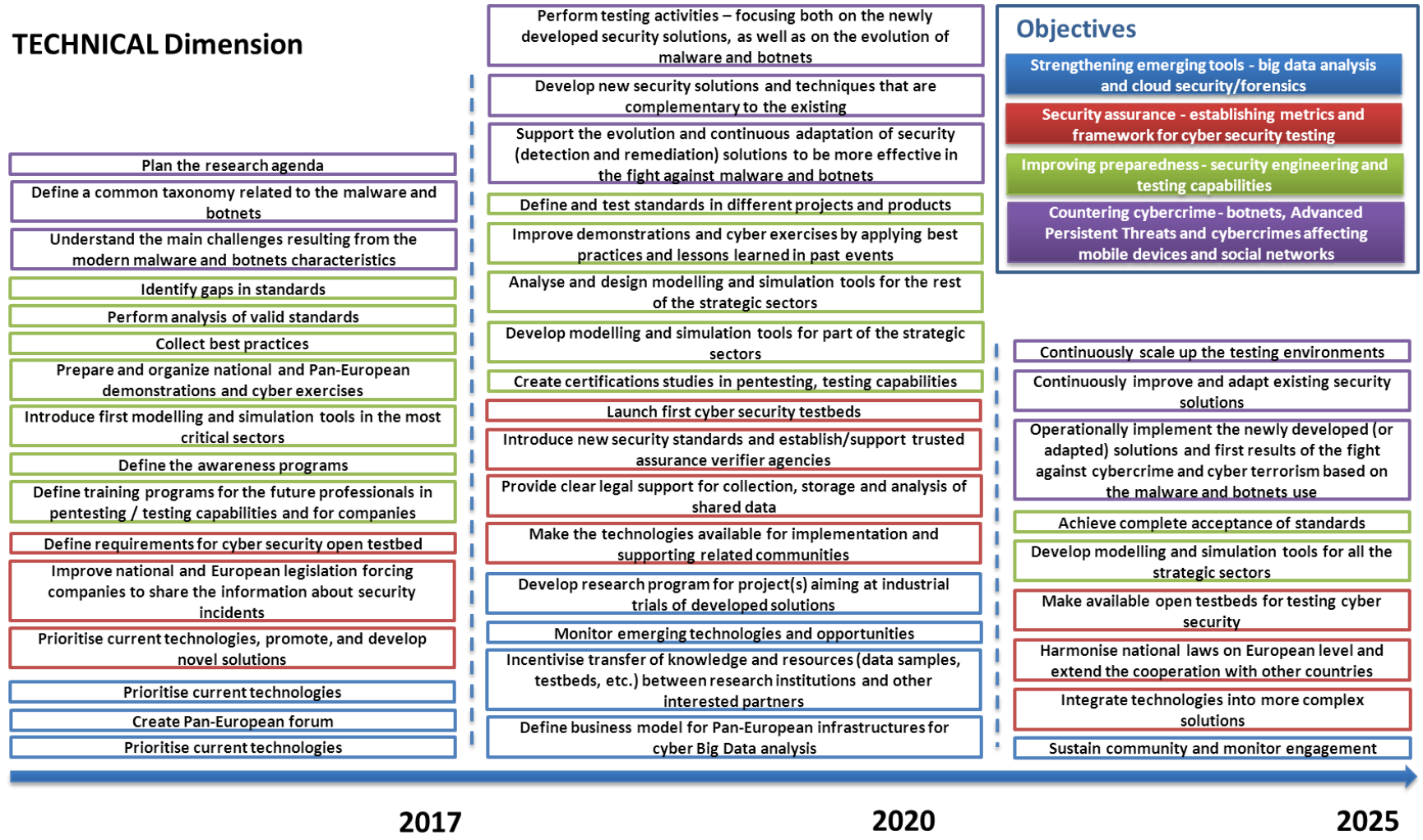

Figure 3: Roadmap activities - Technical dimension

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

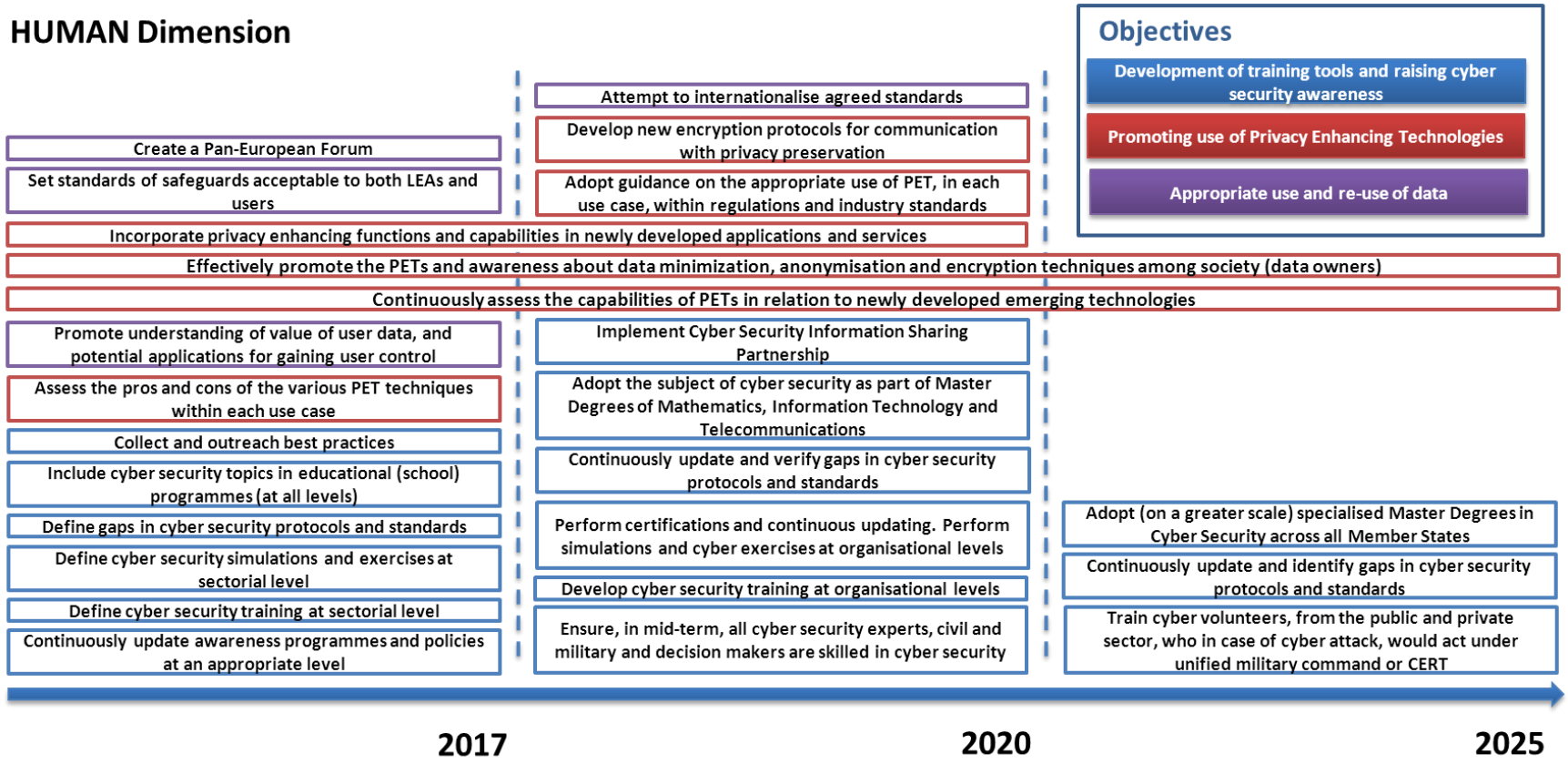

Figure 4: Roadmap activities - Human dimension

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

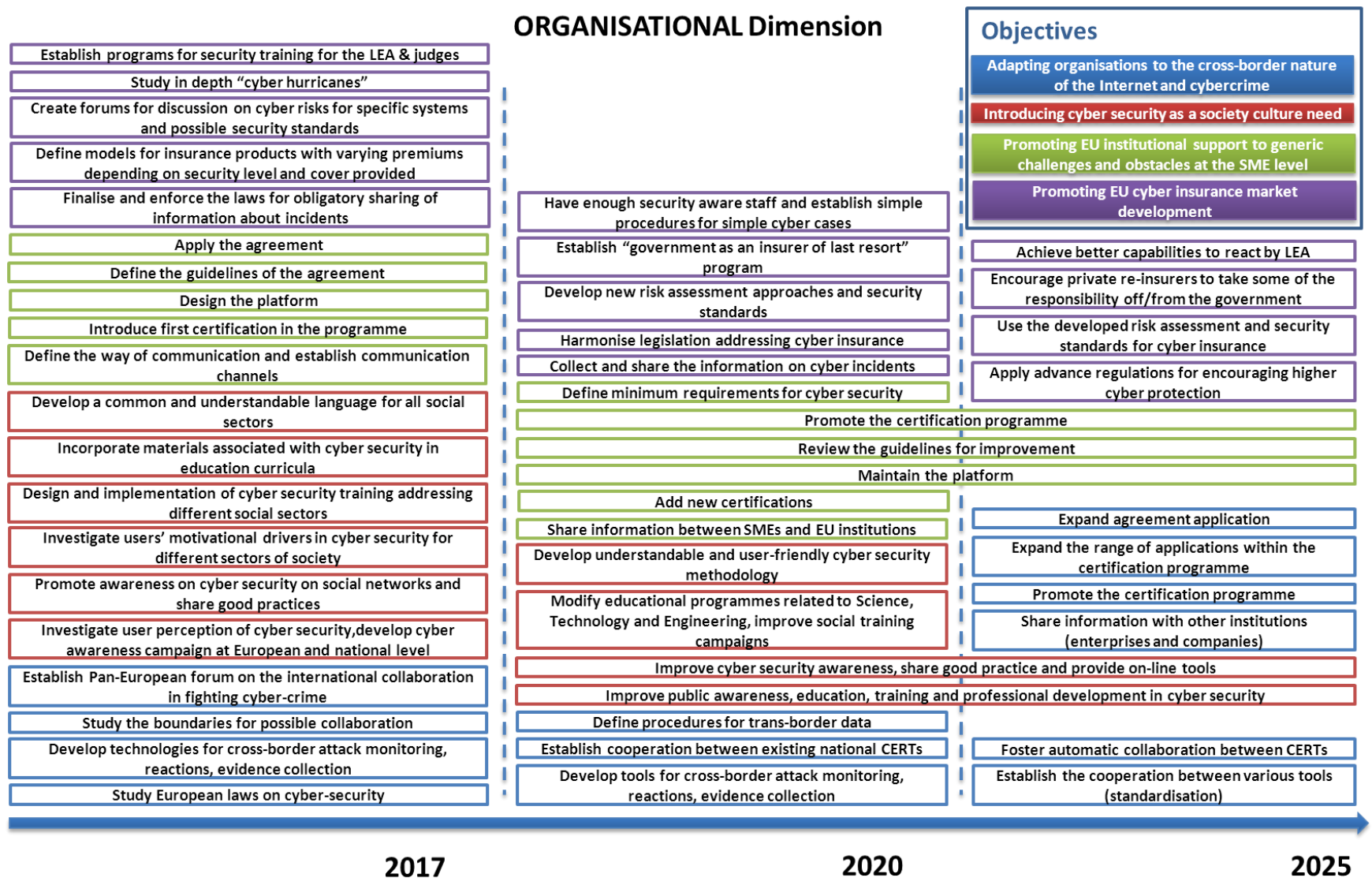

Figure 5: Roadmap activities - Organisational dimension

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

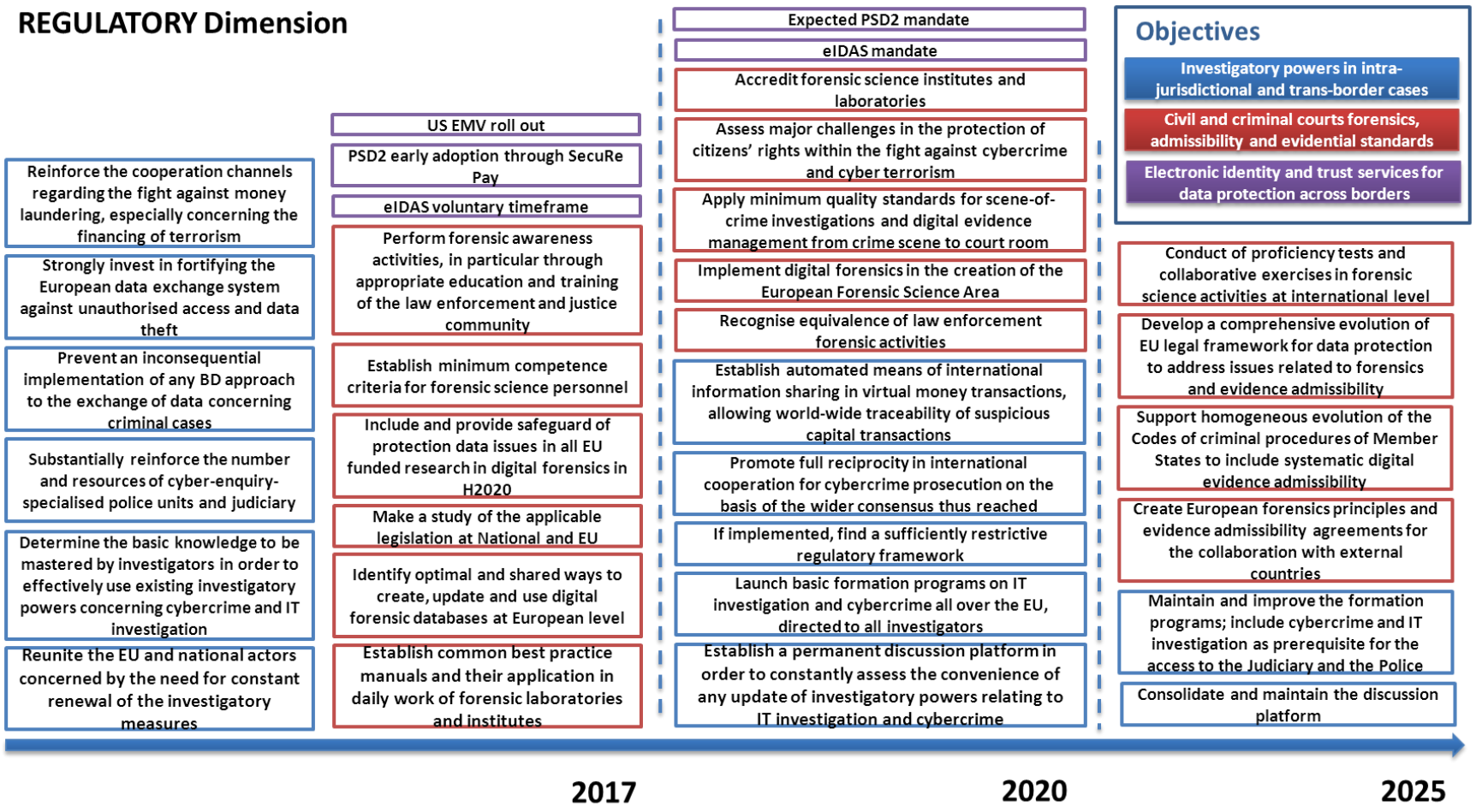

Figure 6: Roadmap activities - Regulatory dimension

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

In M24 we delivered also D4.2 (CAMINO guidelines – final version) document in which the final arrangement of practical guidelines for fighting cybercrime and cyber terrorism is provided.

The CAMINO guidelines address the following target audience:

- Law Enforcement Agencies (LEA),
- Small and Medium Enterprises (SME),
- Citizens/society,
- Public bodies,
- Standardisation bodies.

The respective recommendations for each group of stakeholders is provided according to the specificity and needs for fighting cybercrime and cyber terrorism of the given target group. In particular, different end-user groups have different tools to improve general resistance to cybercrime and cyber terrorism activities and these are reflected in the guidelines.

In general, the document includes over 50 practical guidelines.

These CAMINO guidelines can be used and implemented by SMEs and citizens to improve their cyber security and resilience with respect to cybercrime. Moreover, the guidelines should help LEAs to counter cybercrime and cyber terrorism. Finally, CAMINO guidelines can also be used to create national doctrines, strategies and recommendations (e.g. by institutions like Ministry of Digitalization or National Security Bureau in Poland).

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

4. THE POTENTIAL IMPACT

The CAMINO project strategic and detailed objectives in particular led to project results which address expected impacts of the 6th Security Call of the FP7 Work Programme, namely:

- Enhancing the surveillance of cyber crime
- Ensuring the security of citizens and critical infrastructures against cyber threats

CAMINO highly impacts policy makers and law enforcement agencies (LEAs) and provided them with information about the cybercrime, cyber terrorism and protection measures and recommendations.

Therefore, CAMINO impacts all entities that use IT technologies and are potential victims of cybercrime. It should be emphasised that the CAMINO roadmap can now be used by national funding agencies, by the EC to structure future calls, by ENISA, EDA, etc. Also, it can be (and already is) used by national bodies working on national doctrines and strategies (such as the Ministry of Digitalization and National Security Bureau in Poland). The suggested research items are also targeted at the cyber PPP board in order to help structure the future cPPP initiatives.

The CAMINO roadmap is already acknowledged/mentioned in the ENISA working document: Aligning research programme with policy - Recommendations in the specialised area of NIS from May 2016.

As IT technologies are incorporated in every branch of industry and all spheres of life, they could be impacted by the CAMINO project results. Guidelines and recommendations provided by the project can be applied anywhere where cyber threats and cybercrime are performed, i.e. cyber security at national, governmental, local level, at industrial, financial, business, educational level.

Those impacts by the project can be divided into the following groups of potential beneficiaries:

- End-users (such as law enforcement agencies) - by providing them with guidelines and recommendations to be implemented in the area of cyber security, as well as knowledge about current cyber threats and protection mechanisms to be used by decision makers;
- SMEs – through developing a roadmap for dealing with cyber security, which can be used for future contracts with their customers (e.g. local administration, crisis management centres, power, communication of financial sector) and for further expansion of their services;
- Cyber Security related consulting companies;
- Industry (Cyber Defence Service providers and Product Suppliers) - by providing them with guidelines and recommendations as well as knowledge about current cyber threats and protection mechanisms, which can be applied in their internal projects and applications, and then can be sold/offered to third-party customers;
- CERTs;
- Public administration and Homeland security;
- Associations of information security professionals, e.g. the Institute of Information Security Professionals, the International Information Systems Security Certification Consortium or ISACA;

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Stakeholders, Experts and Supporting Members can also benefit from the CAMINO project. They were the first recipients of the information about project results, analysis and recommendations.

Project impact can be considered also at the European level and in economic as well as societal dimension.

4.1 Impact on stakeholders: workshops, seminars and consultations

According to DOW, WP3 devoted to organisation of workshops, seminars and consultations, started at Month 4. During the whole project lifetime, WP3 progress was perfectly aligned with the work plan and all the objectives and Key Performance Indicators defined for workshops organisation were achieved.

According to DoW, we planned at least four project workshops. Finally, CAMINO Consortium prepared and conducted seven events for cyber security experts. The final list of workshops organised by CAMINO, including the additional CAMINO workshop for the CAMINO Cyber Think-Tank and Supporting members, as well as a date and location of the final CAMINO workshop are presented in Table 3.

Table 3: Plan of CAMINO workshops.

Event	Location	Date
1st CAMINO workshop	Bern, Switzerland	September 18th, 2014
2nd CAMINO workshop at Mobile World Congress	Barcelona, Spain	March 3rd, 2015
Joint CAMINO-COURAGE workshop	Montpellier, France	April 8th-9th, 2015
3rd CAMINO workshop	London, England	June 15th-16th, 2015
Workshop for SM and Think-Tank members	Warsaw, Poland	19th January 2016
Final CAMINO workshop	San Sebastian, Spain	3th March 2016
COURAGE–CAMINO–CyberROAD joint conference	The Hague, the Netherlands	10th-11th Mach 2016

4.2 Impact on research communities – project dissemination

4.2.1 CAMINO webpage

The domain for the webpage was reserved by ITTI at the negotiations stage.

The website is available online at: http://www.fp7-camino.eu/

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The potential for the CAMINO website to disseminate the project results and achievements can be quantified by the statistic information about the website traffic and traffic sources. The figures below present the distribution of website visits during the project and the geographical reach of the visitors. Charts have been created based on website traffic information from period between May 2014 (the month of the website launching) and April 2016.

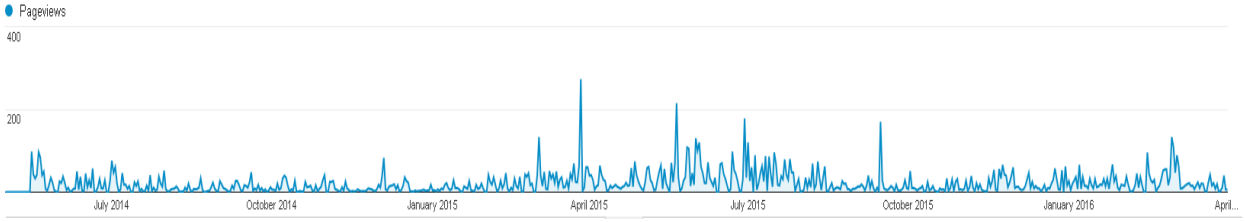

Figure 7: CAMINO website page views over time

The total number of page views is above 15000, including ca. 8200 unique visitors. It is worth noticing, that we continued to have new users of the website (average 3-5 new visitors per day) from outside of the CAMINO Consortium. In addition it should be noted that CAMINO events (e.g. first CAMINO workshop) are interrelated to increased website traffic. Noticeable peaks of pageviews in the April and July 2015, as well as in March 2016 were related to the CAMINO workshops, reaching almost 200 pageviews per single day (Figure 7). Significant increase of the pageviews in the March/April 2015 and March 2016 is also related to the intensification of the project dissemination activities.

The geographical range of the unique visitors of the CAMINO website is very broad, including e.g. Poland, France, Spain, UK and USA with above 500 pageviews from each of these countries. The other countries from the website views which were frequent are Italy, Germany and Ireland. However, countries such as Canada, Malaysia, South Korea, Singapore, etc., are also represented within the website visitors, therefore CAMINO was promoted and has reached countries beyond the European Union boundaries

4.2.2 Social media

One of the major WP5 activities is online presence of the CAMINO, e.g. via social media. So far we used the following social media channels:

- Twitter (https://twitter.com/FP7_Camino)
- LinkedIn
- YouTube (we have already used DFRC YouTube channel for WS1 and WS2 dissemination), but the consortium has decided to create a dedicated channel for the project.

Twitter

CAMINO Twitter account was used to inform about relevant activities related to the project, not only internal activities (results, events, etc.) but also news or activities related to the fight against cybercrime and cyber terrorism. The different relevant activities regarding CAMINO itself or other cybercrime and cyber security issues are being sent to CAMINO channel by the different partners. For example, the

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

CAMINO workshop in London was broadcasted in real time using the CAMINO Twitter account. All the different speakers and main highlights were published.

The CAMINO Twitter account is @FP7_Camino , the CAMINO Twitter account is also embedded into the project website (http://www.fp7-camino.eu/), so that the tweets can be visible there.

In total, we have almost 70 followers of the CAMINO Twitter account and during the project we posted over 60 tweets about the project news.

LinkedIn

As LinkedIn is a business-oriented social networking service, it was a useful tool to reach different stakeholders and therefore, gather information about the CAMINO impact amongst the community.

A CAMINO LinkedIn group was set up, in order to involve the LinkedIn community through news and discussions. The URL of this page is https://www.linkedin.com/groups/8125635

The LinkedIn group has achieved over 40 members. Different news and discussions related to cybercrime are posted here.

YouTube

In order to centralise the videos produced by partners related to the project, a CAMINO video channel was created on YouTube, the leading video channel on the Internet.

The URL is https://www.youtube.com/channel/UCPfUQqwk0JTGOUx9EWtKx1Q

4.2.3 Dissemination events and conferences

The project outcomes have been disseminated through different events and conferences related to the fight against cybercrime. Within these events, one of them is especially relevant, namely, the Final CAMINO Workshop, where all research during the life of the project was presented. The following events were attended by CAMINO partners to disseminate the project during the project:

- IMG-S TA7 group at the meeting in Athens,
- At EDA at the meeting concerning Cyber Situational Awareness (Brussels, June 2014),
- Cyber Conflict Conference, NATO CCDCOE (Tallinn, June 2014)
- TAPT “ICT Crime” workshop (Szczytno, June 2014),
- KYBERTURVALLISUUS – Cyber Security (Jyväskylä, September 2014)
- 1st CAMINO Workshop (Bern, September 2014)
- CYSPA project launch (Berlin, September 2014)
- InfoBalt FISC Workshop (Vilnius, October 2014)
- III Industrial Cybersecurity Congress (Madrid, October 2014)
- SECURE Conference (Warsaw, October 2014)

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- International Conference and Exhibition "Cyber security threats – Safety and security above borders" (Warsaw, November 2014)
- CyberCrime Conference (Tallinn, November 2014)
- SESOCUKR – International Conference on Secure Society (Kiev, November 2014)
- CPExpo & SRC Security Research Conference (Genova, December 2014)
- E-Crime workshop (Rome, January 2015)
- Conference "System for Prevention and Combating Cybercrime" (Warsaw, February 2015)
- EIF High-Level Round Table (Barcelona, March 2015)
- 2nd CAMINO Workshop at MWC (Barcelona, March 2015)
- 5th International Exhibition of Security & Defence Technologies – HOMSEC (Madrid, March 2015)
- Cyber Attacks (Toruń, March 2015)
- CAMINO-COURAGE Joint Workshop "Innovation and cybercrime: challenges of the digital transformation in Europe" – April 2015
- Technical Aspects of ICT Crime (TAPT) Conference in Szczytno (organised by WSPol) – June 2015
- CAMINO Workshop in London – June 2015
- CyberGOV conference in Warsaw – June 2015
- International Workshop on Cyber Crime (IWCC 2015) in Toulouse – August 2015
- Cybersec 2015 conference in Warsaw – September 2015
- XIX Conference on Telecommunications and IT Security (SECURE 2015) in Warsaw – October 2015
- NATO funded conference on Critical Infrastructure Protection and Energy Protection in Kiev – October 2015
- Cyberspace Conference 2015 in Brno – November 2015
- CAMINO Workshop for Supporting Members and CAMINO Cyber Think-Tank in Warsaw – January 2016
- 5ª Giornata Programmatica Conference in Rome – January 2016
- Final CAMINO Workshop "Cybercrime and Cyberterrorism Research Summit" in San Sebastian – March 2016
- The COURAGE – CAMINO – CyberROAD joint conference on "Emerging and Current Challenges in Cybercrime and Cyberterrorism" in the Hague – March 2016
- Przeciwdziałanie i zwalczanie cyberprzestępczości (eng. *Countering and fighting against cybercrime)* in Warsaw – March 2016

4.2.4 Scientific Publications

CAMINO partners have also written different papers where the results of the project in terms of the realistic roadmap to counter cybercrime and cyber terrorism are presented. These papers are the following (only papers published after M12 are listed in the table):

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Table 4: CAMINO publications

Type	Date	Description
Publication	November 2014	Choraś M., Kozik R., Machine learning techniques applied to detect cyber attacks on web applications , Logic Journal of the IGPL, vol. 23(1): 45-56, 2015
Publication	May 2015	Choraś M., Młynarek P., Kosiński J., Kozik R., Research and activities of CAMINO Project in the area of countering cyber crime, in: Kosiński J.: ICT Crime (Przestępczość Teleinformatyczna), Szczytno 2014 (written in Polish)
Publication	September 2015	Puchalski D., Choraś M., Kozik R., Hołubowicz W., CAMINO Roadmap for improving resilience against cybercrime and cyber terrorism, in: Kosiński J.: ICT Crime (Przestępczość Teleinformatyczna), Szczytno 2015 (written in Polish)
Publication	August 2015	Choraś M., Kozik R., Torres Bruna M.P., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A., Comprehensive Approach to Increase Cyber Security and Resielience , in Proc. of ARES (International Conference on Availability, Reliability and Security), 686-692, Touluse, August 2015, IEEE.
Publication	October 2015	Puchalski D., Choraś M., FP7 CAMINO Roadmap, CIIP Focus, no. 10, 13-15, 2015 (written in Polish)
Publication	November 2015	Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. (2015). A Survey on Cyber-Insurance
Publication	July 2016	Choraś M., Kozik R., Churchill A., Yautsiukhin A., Are We Doing All The Right Things To Counter Cybercrime? In Akhgar B., Brewster B. (Eds.): Combatting Cybercrime and Cyberterrorism – Challenges, Trends and Priorities, pp. 279-294, Advanced Sciences and Technologies for Security Applications, Springer, Switzerland, 2016
Publication	July 2016	Choraś M., Kozik R., Maciejewska I., Emerging Cyber-Security: Bio-Inspired Techniques and MITM Detection in IoT, In Akhgar B., Brewster B. (Eds.): Combatting Cybercrime and Cyberterrorism – Challenges, Trends and Priorities, pp. 193-207, Advanced Sciences and Technologies for Security Applications, Springer, Switzerland, 2016
Publication	July 2016	Akhgar B., Choraś M., Brewster B., Bosco F., Vermeersch E., Puchalski D., Wells D., Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism, In Akhgar B., Brewster B. (Eds.): Combatting Cybercrime and Cyberterrorism – Ch allenges, Trends and Priorities, pp. 295-321, Advanced Sciences and Technologies for Security Applications, Springer, Switzerland, 2016
Publication (submitted)	2016	Choraś M., Kozik R., Puchalski D., Hołubowicz W., Aspekty Cyberprzestępczości w Projektach Europejskich – Projekty CIPHER oraz FP7 CAMINO (written in Polish), Cyber Crime in the European Projects – DG Home CIPHER and FP7 CAMINO, submitted to Internal Security Journal

4.2.5 Dissemination materials

Project Presentation

A complete presentation of the project has been produced. It can be downloaded through the following link: http://www.fp7-camino.eu/assets/files/01-Michal_Choras_Workshop-CAMINO-final

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

The content of this presentation includes the following topics:

- Key facts
- Consortium
- Supporting Members
- Project origins
- Project objectives
- Community building
- Cooperation
- Next workshops

Flyer

At the very beginning of the project, a flyer was designed and used for promotional purposes. Once the project progressed and the CAMINO roadmap and guidelines were available, a new flyer was designed to include this information. This new flyer can also be downloaded from the CAMINO website through http://www.fp7-camino.eu/assets/files/CAMINO%20flyer.pdf

CAMINO Roll-up

The CAMINO consortium prepared a printed "roll-up" to be used at various dissemination events after the CAMINO project closed.

CAMINO book and short version of the CAMINO Roadmap (brochure)

Based on the D4.4 CAMINO Roadmap content, the consortium prepared and printed the CAMINO Book entitled: "Comprehensive roadmap (research agenda) for fight against cybercrime and cyber terrorism". An ISBN number has been assigned (ISBN: 978-83-64539-01-5) to the publication. Hardcopies of the book will be used as promotional material at various dissemination events.

The CAMINO consortium also prepared a shortened version of the roadmap (in the form of a 20-page brochure) for easier sharing of the CAMINO roadmap concepts and approach. This version has also been printed using ISBN number (978-83-64539-02-2).

4.3 Community building - project sustainability

From the beginning, the consortium focused on dissemination and community building. All partners started to contact relevant stakeholders and organisations from the start of the project.

In particular, IMG-S (Integrated Mission Group Security) TA7 and IMG-S SCG (Synthesis and Coordination Group) are informed about the results of the CAMINO project.

Also right from the start, we contacted our Supporting Members – those who express the will to support us and signed the letter of support during the proposal stage. The majority of them responded positively, and we are in contact with them (sending updated about project status to the special mailing list). We

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

also contacted organisations such as: Europol, ENLETS, EDA, EU Commission, DG ENTR, Chief Police Office Warszawa, Dutch Ministry of Justice, TNO, E-OS, the European Parliament, UK Parliament, US Executive bodies, Regional Police Offices in Poland, FISC (Finnish Information Security Cluster), Finnish Defence Research Center, numerous industry bodies among others to disseminate CAMINO.

4.3.1 Supporting Members

The CAMINO Supporting Members Group was constituted at the beginning of the project and was formed of several important stakeholders related to the project who collaborated with the CAMINO consortium. It offered advice and guidance to the project in matters belonging to any of the members' competence. Finally, we were supported by 24 cyber security experts from 22 organisations representing 13 countries (including USA).

During the lifetime of the Project, Supporting Members offered their knowledge, experience and guidance, through the attendance at meetings and provided their feedback via mailing lists dedicated to Supporting Members.

Since the Integrated Mission Group for Security (IMG-S) was the starting point of the project, there has also been a strong collaboration with this group, especially IMG-S Technical Area Cyber Security (TA7), as 6 members of CAMINO and 11 Supporting Members are involved in TA7.

4.3.2 CAMINO Think Tank

The CAMINO Think Tank is an initiative whose main objective is the exchange of experience and knowledge, as well as the dissemination of information related to effective measures against cybercrime and cyber terrorism.

CAMINO think tank is an informal initiative – an association of loosely coupled experts, i.e. it has no legal status and was not formally registered, e.g. as a non-profit organisation. Its members want to support national and international decision makers and the EC in the area of cyber security.

The CAMINO think tank followed the comprehensive approach and took into account a variety of dimensions relating to the fighting against cybercrime and cyber terrorism such as technical, human, organisational and legal aspects.

Whoever wants to continue to participate in the CAMINO Think Tank can do it by registering via the CAMINO web page. At the M24, CAMINO Think Tank is composed of 25 cyber security experts from 9 countries.

4.3.3 Towards the Consolidated Roadmap: cooperation with other projects

During the project lifetime, CAMINO has cooperated with two other consortia:

- COURAGE (www.courage-project.eu): The COURAGE project is funded by the European Commission's seventh framework programme for research. COURAGE is producing a research agenda for Cyber Crime and Cyber Terrorism using the expertise of the consortium partners,

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

advisory board members and recruited expert stakeholders. The research agenda will identify the major challenges, reveal research gaps for Cyber Crime and Cyber Terrorism.

- CyberROAD (www.cyberroad-project.eu): CyberROAD 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 cyber-crime and cyber-terrorism in order to draw a strategic roadmap for cyber security research. A detailed snapshot of the technological, social, economic, political, and legal scenario on which cybercrime and cyber terrorism does develop will be first provided.

These projects have cooperated to organise joint workshops. These are the following:

- The CAMINO & COURAGE joint workshop: "Innovation and cybercrime: challenges of the digital transformation in Europe". Montpellier (France), 8-9 April 2015
- The COURAGE – CAMINO – CyberROAD joint conference on "Emerging and Current Challenges in Cybercrime and Cyberterrorism". The Hague (Netherlands), 10-11 March 2016.

The cooperation between the three projects has been very fruitful, with exchanging of ideas and experiences, resulting in the consolidating of the projects outputs (Joint Consolidated Roadmap).

In order to facilitate the consolidation of the three respective research agendas/roadmaps, each project adapted its roadmap content to a normalised, pre-defined format and within an agreed framework. It should be noted that three consortia agreed CAMINO THOR approach with four CAMINO roadmap dimensions as the basis for structure of the new consolidated research agenda.

The categories within which each of the respective research agenda have derived their items fundamentally different in the way, but are however cross-pollinating and thematically consistent in the content they address. The mapping of CAMINO and COURAGE approaches is presented in Table 5.

Table 5: Categories of CAMINO and COURAGE roadmap topics.

		COURAGE					
		Cooperation & Information Exchange	Investigators Capability	Legislative Systems and Regulation	Awareness, Education & Training	Technological Change	Organisational & Societal Resilience
CAMINO	Technical	■	■			■	■
	Organizational	■			■		■
	Human				■	■	
	Regulatory	■	■	■			

The current topics included in the consolidated roadmap are presented in Table 6 with the indication of primary source of the content in respective topics.

The presented roadmap is the version from May 2016, with topics by COURAGE and CAMINO (still awaiting topics from CyberROAD).

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Table 6: Consolidated roadmap - topics.

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

Each respective research agenda item has been adapted to this structure and describes the following characteristics:

- **Specific Challenge -** Provide background information and insights into the problem domain, the specific challenges and issues being faced as a result, and an overview of what the proposed research should address.
- **Scope -** Set the boundary for what the research should aim to achieve and the specific outcomes which are expected/needed of the research in order to sufficiently address the specific challenge previously outlined.
- **Expected Impact(s)** - Outline explicitly the expected beneficiaries of the research, and how it will provide value.
- **Key Objectives -** Provides a set of targeted objectives for the research in line with the expected impacts, scope and specific challenge(s).
- **Timeline for actions** - The provision of short (1-2 years) and medium (5 years) term milestones, in terms of impact and realisation for the each of the research objectives.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

- **Barriers and risks to achievement** - Outline any risks and barriers that exist in relation to the research topic which may prevent the objectives from being achieved, and measures that could be implemented to mitigate them.

Finally, the resulting items have been qualitatively analysed and where appropriate aggregated in order to form the consolidated research roadmap. The final version of the consolidated agenda will be delivered alongside the final delivery of the CyberROAD research agenda in May 2016.

4.4 Adoption and exploitation of the results

In the second year of the project we performed effort towards better adoption of the roadmap and better sustainability of the project results. In this context, it should be emphasised that the CAMINO Think-Tank established during the project is the initiative promoting and enhancing ideas and approaches built during the CAMINO. We expect that after the project, CAMINO Think-Tank will be a complementary initiative for IMG-S TA7, from which CAMINO originates. IMG-S will take the roadmap and will update it (in cooperation with the CAMINO Cyber Think-Tank) when appropriate.

The general timeline for particular initiatives is presented in the Figure 11.

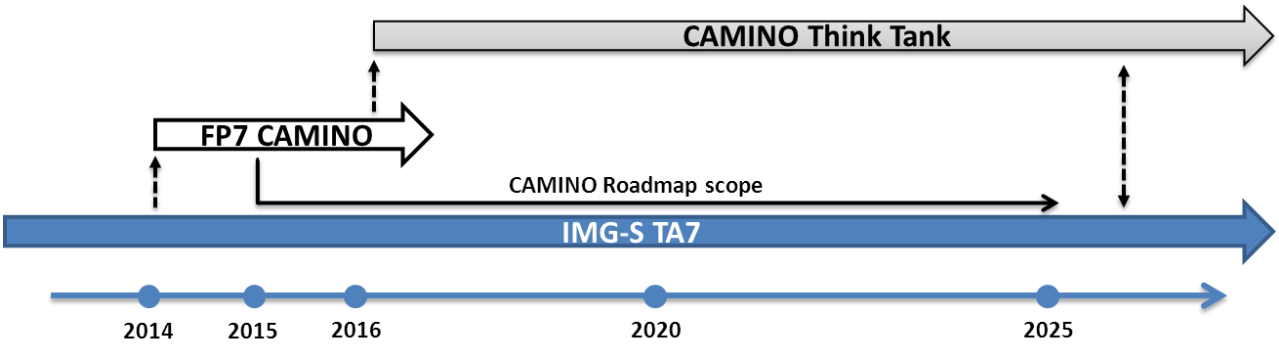

Figure 8: CAMINO Think-Tank - timeline and relation to the CAMINO project and IMG-S initiative

5. ADDRESS OF THE PROJECT PUBLIC WEBSITE

CAMINO project website was created and is maintained by the project coordinating organisation (ITTI) and is available at: www.fp7-camino.eu. **CAMINO webpage has been reserved (paid) by ITTI until 31.07.2017 and at least ITTI plans to update it whenever appropriate after the project finalisation.**

6. PROJECT LOGO, DIAGRAMS OR PHOTOGRAPHS

The project logo (Figure 9) has been designed by ITTI and accepted by the rest of Consortium in the proposal preparation stage.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406

Figure 9: CAMINO logotype.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406