Comprehensive Approach to Increase Cyber Security and Resilience

CAMINO Roadmap and Research Agenda

Michał Choraś[12]
[1] ITTI Sp. z o.o., Poznań, Poland
mchoras@itti.com.pl
[2] University of Science and Technology in Bydgoszcz
chorasm@utp.edu.pl

Rafał Kozik[12]
[1] ITTI Sp. z o.o., Poznań, Poland
rkozik@itti.com.pl
[2] University of Science and Technology in Bydgoszcz
rkozik@utp.edu.pl

María Pilar Torres Bruna
Everis Aeroespacial y Defensa sl,
Madrid, Spain
maria.pilar.torres.bruna@everis.com

Artsiom Yautsiukhin
Consiglio Nazionale delle Ricerche
Pisa, Italy
artsiom.yautsiukhin@iit.cnr.it

Andrew Churchill
CBRNE Ltd
London, United Kingdom
andrew.churchill@cbrneltd.com

Iwona Maciejewska
DFRC AG
Bern, Switzerland
iwona@dfrc.ch

Irene Eguinoa
S21sec
Pamplona, Spain
ieguinoa@s21sec.com

Adel Jomni
Université de Montpellier
Montpellier, France
adel.jomni@gmail.com

Abstract— In this paper the initial results of the European project CAMINO in terms of the realistic roadmap to counter cyber crime and cyber terrorism are presented. The roadmap is built in accordance to so called CAMINO THOR approach, where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory.

Keywords— cyber security, cyber crime, cyber terrorism, roadmap, project CAMINO

I. INTRODUCTION

The major goal of the CAMINO project is to provide a realistic roadmap for improving resilience against cybercrime and cyber terrorism. In other words the project should answer the question where should taxpayer money be invested for research purposes. We indicate what research directions could tackle the problems and mitigate the gaps in countering cyber crime and cyber terrorism in a timescale up to 2025.

The consortium uses a holistic approach, analysing functions and capabilities addressing technical and human issues which are inter-related with legal and ethical aspects. We follow 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.

The project consortium has 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 that will complement LEA and research organisations - without creating a bottleneck of problems and obstructions. More information about the project can be found at: www.fp7-camino.eu/.

In this paper the initial roadmap from March 2015 is presented. The final roadmap will be delivered in March 2016, after year-long consultations in order to reach wide consensus.

This paper is structured as follows: in Section 2 CAMINO THOR approach is overviewed. In Section 3 the results of our analysis of the current situation with regards to cyber crime and cyber terrorism (technologies, challenges, needs) are described. In Section 4 CAMINO roadmap (initial version) items are presented. Each dimension item is shortly described and also the figures showing actions and their timeline are presented. Conclusions are given thereafter.

978-1-4673-6590-1/15 $31.00 © 2015 IEEE
DOI 10.1109/ARES.2015.30

II. CAMINO APPROACH

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 cyber crime and cyber terrorism,
- (H)uman – related to hum*an factors, behavioral aspects,* privacy issues, as well as raising awareness and knowledge of society with regards to cyber crime 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.

Visualisation of the THOR approach in the CAMINO project is presented in Figure 1.

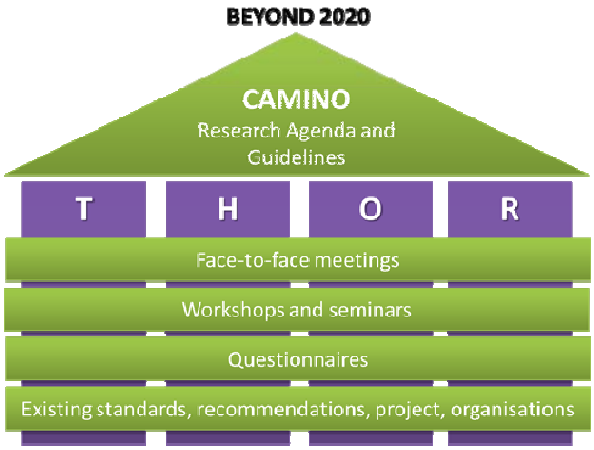

Figure 1. THOR approach for the CAMINO project

III. ANALYSIS RESULTS

Current roadmapping initiatives with identification of main research gaps and challenges were the subject of analyses performed in the initial stage of the CAMINO project. This section is focused on the presentation of main conclusions formulated in the CAMINO WP2 documents to summarise key areas, technologies and threats impacting cyber crime and cyber terrorism nowadays.

Firstly, we analysed a number of cyber security roadmaps (also sector-specific ones), current and already completed R&D projects and international strategies [1]-[11]. The common aspects that are discussed in these documents and analysed in various projects are:

- Evaluation of system security,
- Identity management,
- Improvements of analytical tools for security monitoring,
- Security-related information sharing mechanisms,
- Increasing of the security awareness,
- Standardisation in the field of cyber security,
- Application of Security/Privacy-by-design principles,
- Critical Infrastructure Protection.

These topics were our starting point while defining the CAMINO roadmap scope.

In the early phase of the project we analysed also risks related to the various classes of assets. In result, we diagnosed that payment systems (financial and banking domain), embedded systems, cloud computing services and systems processing personal data are particularly vulnerable to the cyber crime and cyber terrorism threats. Therefore, protection of these assets is addressed by particular parts (topics and objectives) of this roadmap. Also, means to reduce risks connected to these assets are reflected by the milestones defined in the proposed research agenda timeline.

The study about the cyber security technologies state of the art allowed us to identify several key areas that due to their emerging status and maturity level should be particularly addressed by the roadmap. Those are:

- 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.

Finally, in WP2 (and through WP3 workshops) we performed a number of surveys and face-to-face interviews with experts from different sectors related with cyber security and the fight against cyber crime and cyber terrorism.

IV. CAMINO ROADMAP

In this section we present the Roadmap topics divided into four THOR dimensions. In Figures 2 - 5 the activities proposed in the roadmap are presented for each of dimensions and for different time spans: short- (until 2017), medium- (until 2020) and long-perspective (until 2025).

A. Roadmap Topics – Technical Dimension

1) Strengthening/Adapting emerging tools - Big Data analysis and cloud security/forensics

Cyber attacks may not be visible in a small scale, due to their nature or intensity (e.g., amount of traffic they introduce). Therefore, recently techniques using big data tools have been adapted. The recent research shows that the deep analysis of large volumes of data (received from different segments of IT networks) has a unique capability of revealing interesting patterns. This concept is recently adapted to many cyber security areas, namely: spam detection, botnets detection, malwares analysis, web-based infection, network intrusion detection systems.

2) Security assurance - improvements in authentication and authorisation, trust management and information sharing

The IT world becomes more dynamic, distributed and heterogeneous. This evolution implies novel security challenges, especially for security assurance. New methods for authentication, authorisation and trust management have to deal with lack of pre-defined trust assignments and be ready to establish new relations on the fly. Moreover, establishing such relations requires reliable knowledge about previously unknown parties. This observation is also applied to security, in order to ensure the clients that outsourced business will not be compromised even when it is under control of partners. In order to achieve this, information about occurred incidents should be shared. The shared information can be used to get correct assessment of security of an organisation, issue an insurance policy and strengthen the security of the Internet as a whole.

3) Improving preparedness - security engineering and testing capabilities

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 developer team confidence in their system, 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.

4) Countering cyber crime - botnets, Advanced Persistent Threats and cyber crimes affecting mobile devices and social networks

Nowadays, one of the main challenges affecting countering cyber crime 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 cyber crime. This is particularly important in the context of limitations of existing signature-based scanners and malware detectors. On the other hand, cyber crime 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 cyber attacks in conjunction with growing popularity of IoT (Internet of Things) concept.

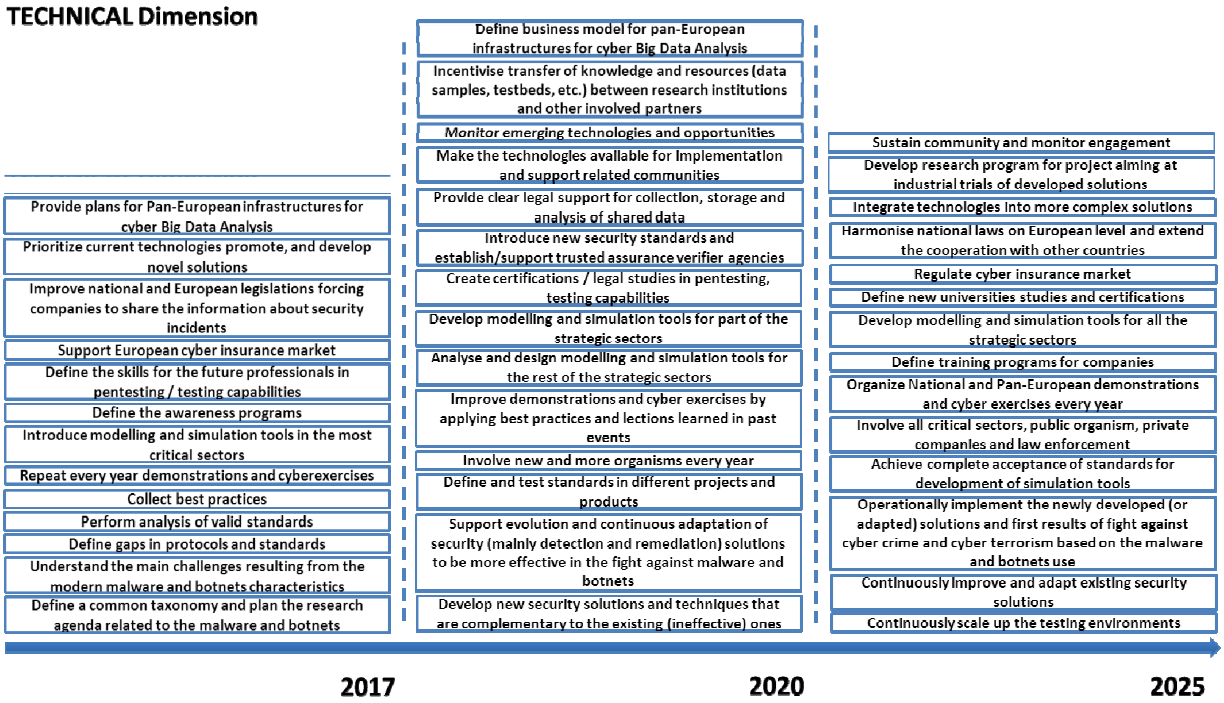

Figure 2. Roadmap activities – Technical Dimension

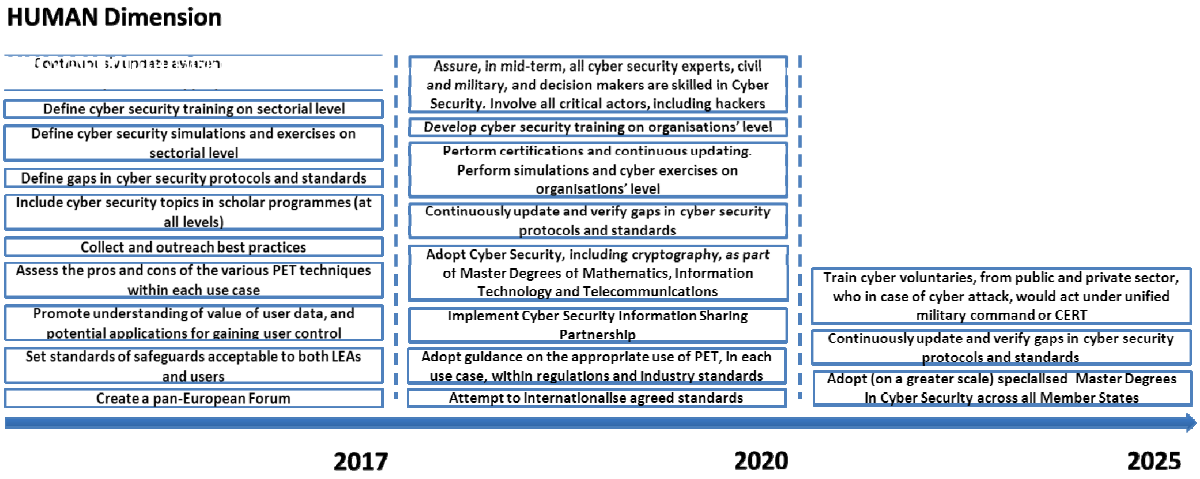

Figure 3. Roadmap activities – Human Dimension

B. *Human activities overview*

1) Development of Training and Awareness tools

One of the most fundamental aspects of improving society's defences against cybercrime, as with protecting against any other new and evolving threat, is to ensure that the users and subjects of it are properly kept abreast of the nature of the threat itself and the underlying rationale of the defensive steps being taken to mitigate it.

Whilst almost all new legislative changes are accompanied by training and awareness strands as part of their lifecycle, few technological changes sufficiently incorporate this vital feature into their own roadmaps. This is true both of the new possibilities opened up through greater online access to data, but also to the tools being rolled out to support the intended security behind them.

2) Utilising 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.

3) Appropriate use and re-use of Data

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 (see under Technical, above), 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.

C. *Organisational activities overview*

1) Adapting organisations to the cross-border nature of the Internet and Cybercrime/Terrorism

Nowadays, the competitiveness is global, so any company may receive an attack from anywhere of the planet. Now, not only the companies that are closely may be interested in the intellectual property or company information. Therefore, most important Regulation differences between countries should be known, and in consequence organisations should be aware of this fact and protect their assets and intellectual taking this into account. Therefore, organisations need to think cross-border regarding cybercrime and protect their networks thinking globally and cooperate to improve the IT security worldwide.

2) Introducing Cyber security as a society culture need

The use of new technologies is now present in the office and at home, at professional level but also for free time, for children and adults, and also to interact with public sector, with banks, supermarkets and online stores. Moreover, these different scopes overlap, and initiatives such as BYOD (Bring Your Own Device) are becoming more popular every year, mixing personal with professional area. Therefore, cyber security is now crucial in terms of securing all aspects in the day-to-day, and it must be introduced as a new culture need.

3) Promoting EU Institutional support to Generic Challenges and Obstacles at the Enterprise / Company / SME Level

A common / unified institutional support is needed to promote changes at the Enterprise / company and SME level. The creation of an experts committee at the request of the main involved countries would contribute to overcome these obstacles and challenges at a European level. In addition, an information sharing platform would help the approach and collaboration of every interested party, making quick and efficient ideas/problems sharing possible. This support will assure the minimum protection needed in these organisms.

D. Regulatory activities overview

1) Investigatory Powers in intra-jurisdictional & trans-border cases

Steps must be taken to adequate investigatory powers, as well as their use by LEA (Law Enforcement Agencies) members, to cyber-enquiries: the pace of regulatory reforms, the balance between abstraction and concretion of the investigatory powers and the need for a training policy are to be taken into consideration. Effectiveness of international cooperation in trans-border cases, paramount to successfully prosecute cybercrime, may be augmented in the years to come if the EU takes advantage of the shift in the views on reciprocity issues by key players such as China. Then again, improved data exchange between EU and National LEA's comes not without a risk for Fundamental Rights, one of the keystones of European culture: efforts must be made in order to find a regulatory and technical framework allowing to juggle augmented data exchange capabilities and respect of Fundamental Rights.

2) Interoperability of Common and Roman Law

Having noted the transnational and intra-jurisdictional nature of cyber crime, one of the key factors to determine in gaining a better understanding of where such crimes might best be prosecuted. Over and above the differences in the definitions of offences, or admissibility of evidence, consideration also needs to be given as to whether there are any noticeable advantages or disadvantages associated with the underpinning legal framework. Our regulatory roadmap will seek to identify such differentials taking account of potentially speedier developments in some international fora, such as Interpol.

3) Civil and Criminal Courts forensics/admissability/evidential standards

At present, there exists a wide variety of standards and best practices for information security and digital evidence gathering. This variety hinders the adoption of common standards and procedures which lay strong foundations for a cooperative and effective fight against cyber crime and cyber terrorism at pan-European level. This type of crime is particularly decentralised and not restricted to any frontier, and the admissibility of digital evidences in Courts is still sometimes dependent on case-by-case analysis by experts who lack a common reference framework. Thus, the challenge is to achieve common understanding and adapt accordingly the current Member States criminal procedures. The achievement of a European Forensic Science Area has become a priority for the European Union. Last but not least, the respect for fundamental rights and freedoms of citizens must always be kept as a basic and key principle.

4) Identity/Authentication Standards for Data Protection across borders

A majority of classes and applications of Cyber Crime and Terrorism contain a misrepresentation of identity or attempt to authenticate for access to goods or services that the attacker has no legitimate use to. There currently exist a plethora of standards to identify and authenticate a genuine user is who he or she claims to be, and their access rights in the given circumstances. At present there is no interoperability of these, and poor controls over the degree to what constitutes 'strong authentication' sufficient for each application. Within the European Union, however, the eIDentity, Authentication & Signatures Regulation, launched in October 2014 seeks to address this. Our Roadmap will take account of the timetable for its implementation, and the necessary external steps necessary to ensure best effect can be taken from it 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 for one of the key cybercrime asset classes, and one of the most likely candidates for higher level eIDAS requirements. The European Central Bank and European Banking Association's announcement on 19th December 2014 that Secure Retail Payment (SecuRe Pay) Strong Authentication requirements would be put in place from 1st August 2015, several years in advance of PSD2's expected ratification, let alone mandated implementation, goes to show how quickly cybercrime and the standards to address it move.

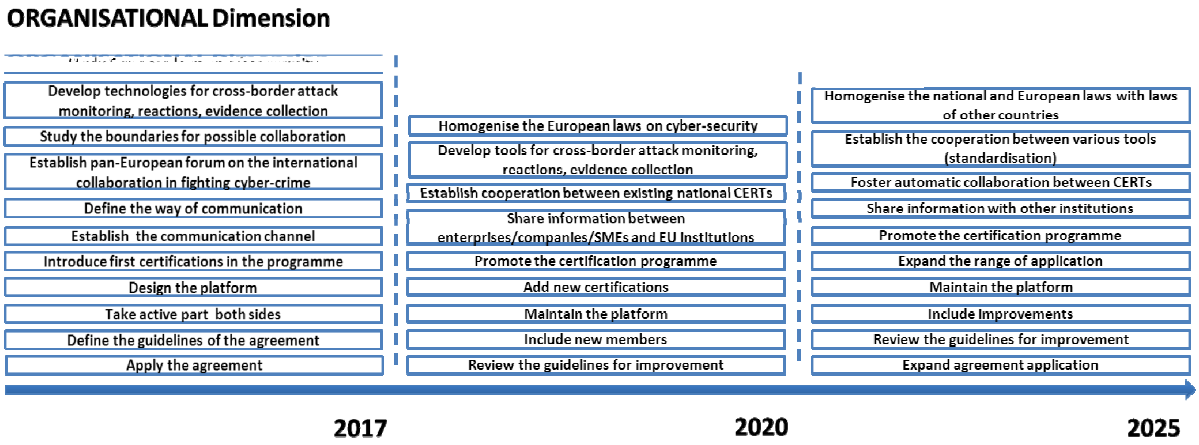

Figure 4. Roadmap activities – Organisational Dimension

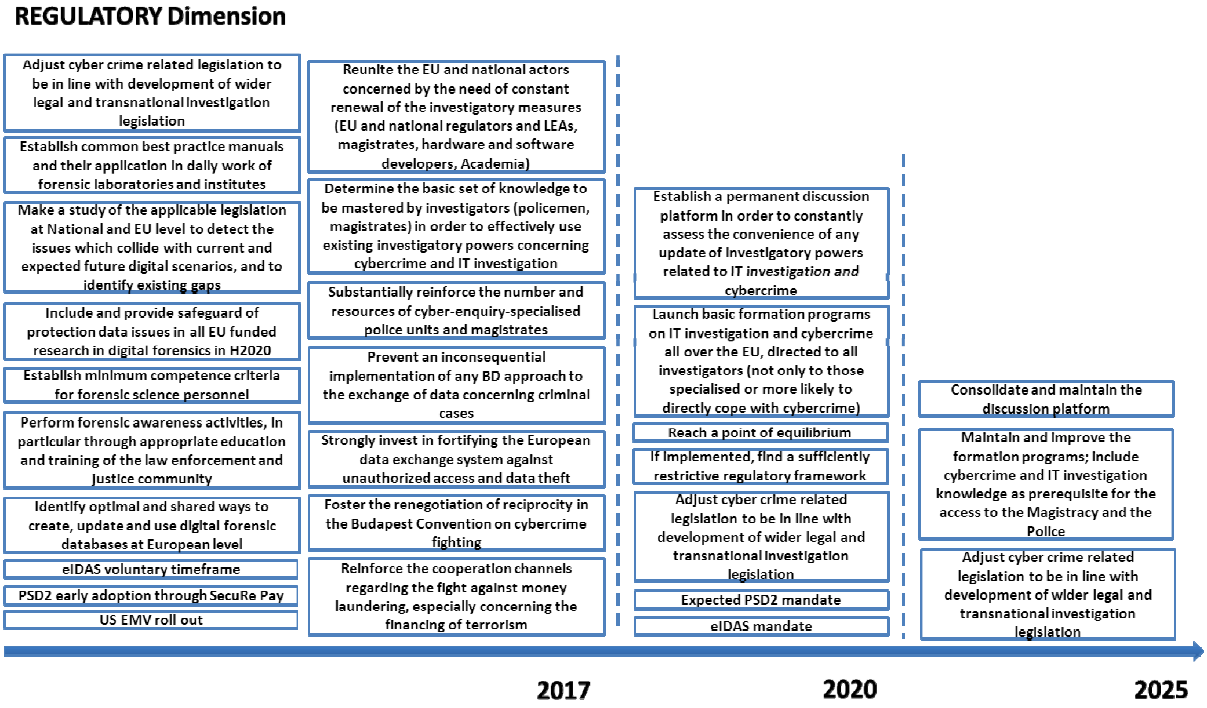

Figure 5. Roadmap activities – Regulatory Dimension

V. CONCLUSIONS

In this paper we presented the cyber security research agenda (the CAMINO roadmap) specifying our suggestions related to the future efforts in fighting against cyber crime and cyber terrorism. The roadmap is focused on four key pillars of cyber security research, presenting the main objectives, problems, challenges and associated stakeholders from each dimension: Technical, Human, Organisational and Regulatory. These four dimensions constitute the CAMINO THOR approach that is basis for this roadmap, as well as for other research activities performed during the whole project.

Each of four THOR dimensions has been described in the roadmaps following the same structure. Firstly, the top priority areas (topics) in THOR dimensions have been defined. In general, there are 14 key topics in the CAMINO roadmap. Topics from Technical part are focused on big data and forensic aspects, improvement of authentication/authorisation mechanisms, security engineering and testing capabilities, as well as on means to effective fight against malware, botnets and APTs (Advanced Persistent Threats). Human dimension emphasises need for mechanisms regulating use and reuse of personal data and for training and raising cyber security awareness. Topics from Organisational part of the roadmap are focused on societal and cultural aspects of cyber security, on adaptation of the organisations in the

light of international nature of cyber crime and cyber terrorism, as well as on cooperation between organisations (e.g. SMEs) and supporting EU institutions. Finally, Regulatory dimension are composed of the following topics: investigatory powers aspects, interoperability of Common and Roman code law, forensics and evidential standards, as well as standards for data protection across borders.

For each topic, the roadmap specifies a number of objectives with assigned milestones and actions to achieve those milestones.

Totally, we have almost 60 objectives and about 300 milestones that are considered as micro-steps in our research agenda, leading to more effective fight against cyber crime and cyber terrorism until 2025. The CAMINO roadmap structure is presented in the Figure 6 (red blocks are additions planned for the second year of the CAMINO duration).

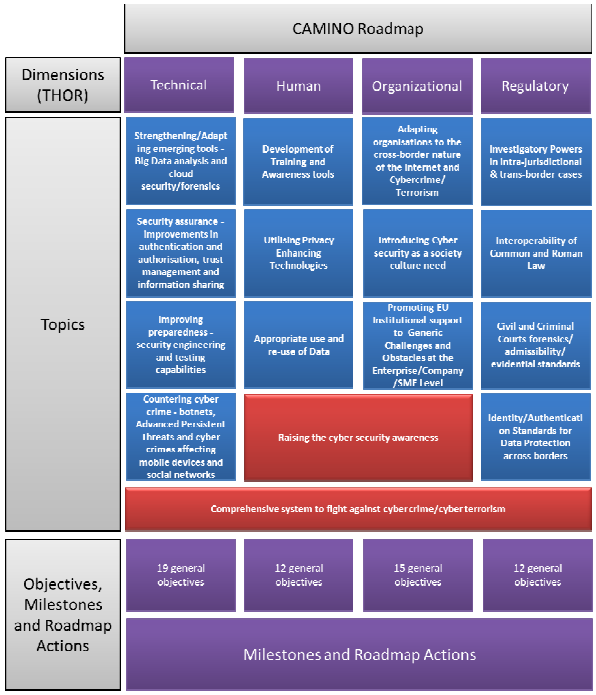

Figure 6. Structure of the CAMINO roadmap.

Our idea is to assure wide consensus and agreement on the CAMINO roadmap suggestions within relevant experts and stakeholders groups.

Therefore, the initial roadmap will be discussed and validated with the experts. In particular it has been or will be presented in the following events:

- CAMINO session at MWC in Barcelona (March),
- Cyber attacks 2015 conference in Torun (March),
- Closed meeting of CAMINO with COURAGE (April),
- CAMINO-COURAGE workshop in Montpellier (April),
- CAMINO workshop in London (June),
- ICT crime conference in Szczytno (June).

During the second year of the CAMINO project duration we plan to specify existing points in the research agenda and to add new ones to make the CAMINO roadmap more complete. In particular we plan to add new cross-domain topics, namely: Comprehensive system to fight cyber crime and cyber terrorism, and raising the cyber security awareness.

ACKNOWLEDGEMENT

This work is partly funded by the European Commission under grant number FP7-607406-CAMINO. The support is gratefully acknowledged.

REFERENCES

[1] U.S. Department of Homeland Security, "A Roadmap for Cybersecurity Research", November 2009.

[2] Evangelos Markatos, Davide Balzarotti, "The Red Book: A Roadmap for Systems Security Research", SysSec (FP7 NoE Project), August 2013.

[3] NIST (National Institute of Standards and Technology), "NIST Roadmap for Improving Critical Infrastructure Cybersecurity", February 2014.

[4] Perry Pederson, Tim Roxey, Jeff Gray, "Cross-sector Roadmap for Cybersecurity of Control Systems", ICSJWG (Industrial Control Systems Joint Working Group), September 2011.

[5] Katie Jereza et al., "Roadmap to Achieve Energy Delivery Systems Cybersecurity", ESCSWG (Energy Sector Control Systems Working Group), September 2011.

[6] U.S. Department of Homeland Security, "Dams Sector Roadmap to Secure Control Systems", 2010.

[7] Jeffrey Berenson, et al. "The Roadmap to Secure Control System in the Transportation Sector", The Roadmap to Secure Control Systems in the Transportation Sector Working Group, August 2012.

[8] Jack Eisenhauer, Paget Donnelly, Mark Ellis, Michael O'Brien, "Roadmap to Secure Control Systems in the Energy Sector", U.S. Department of Energy, U.S. Department of Homeland Security, January 2006.

[9] Seth Johnson, Bruce Larson, Dave Edwards, Kevin Morley, "Roadmap to Secure Control Systems in the Water Sector", Water Sector Coordinating Council Cyber Security Working Group (WSCCCWG), March 2008.

[10] ENISA website, National Cyber Security Strategies in the World, Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[11] EU NIS Platform Working Group 3, Secure ICT Research Landscape Deliverable, July 2014, Available at: https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/state-of-the-art-of-the-secure-ict-landscape/at_download/file