Comprehensive Approach to cyber roadMap coordInation and deveLOpment

CAMINO roadmap (research agenda) for fight against cybercrime and cyber terrorism

www.fp7-camino.eu
Date of the document: 31/03/2016
Document title: CAMINO roadmap (research agenda) for fight against cybercrime and cyber terrorism

Responsible beneficiary: ITTI Sp. z o.o.
Editors: Michał Choraś and Rafał Kozik (ITTI Sp. z o.o.)
Contributing beneficiaries: ITTI Sp. z o.o., CBRNE Ltd., Consiglio Nazionale delle Ricerche, Data Fusion Research Center AG, Espion Ltd., Everis Aeroespacial y Defensa S.L., Montpellier University, Police Academy in Szczyno, S21sec Information Security Labs S.L., Sec-Control Finland Ltd.

ISBN: 978-83-64539-02-2
*** This page is intentionally left blank ***
**MEET THE PROJECT**

The major goal of the project was to provide a realistic roadmap for improving resilience against cybercrime and cyber terrorism.

The consortium has its roots with the Integrated Mission Group Security (IMG-S) Cyber Theme Area, where the cyber security partners have an extensive experience in developing roadmaps. The participation of the Supporting Members in the CAMINO project, coming from Europe and North America (USA and Canada), ensured that the roadmap benefits from the vast knowledge and experience. The consortium have a very practical approach, with most partners being SMEs with a good understanding of what is realistic and practical and with an interest in finding a constructive roadmap complementing LEA and research organisations — without creating a bottleneck of problems and obstructions.

The consortium used a holistic approach, analysing functions and capabilities addressing technical and human issues which are inter-related with legal and ethical aspects. We followed so called CAMINO THOR approach where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory. In each of the dimensions some items are proposed for the roadmap. In parallel with looking at the human and technical aspects, the project is focused on strong involvement of various different groups and operators such as LEAs, CERTS, personal users, governments, industry and research and commercial organisations.

During the project we developed the CAMINO roadmap (research agenda). For each THOR dimension we identified 3-4 top priority topics that have to be addressed to more effectively fight against cyber crime and cyber terrorism. Each of these topics is described in the roadmap and is presented in the unified way. Topic description includes summary of key research objectives, summary of stakeholders with their roles in relation to given topic and detailed timeline. In this timeline we specified concrete milestones for three different time-spans (2017, 2020 and 2025). Such timelines briefly explain also current situation in given topic and expected (desired) end-vision at 2025, after the roadmap milestones achievement. Finally, topic timelines include summary of research activities that should be performed, leading to the defined milestones achievement.

Also, we constituted the CAMINO Cyber Think-Tank. Its main objective is the exchange of experience and knowledge, as well as the dissemination of information related to the effective measures against cyber crime and cyber terrorism. Its members would like to support national and international decision makers and EC in the area of cyber security.
OUR APPROACH – METHODOLOGY & THOR EXPLANATION

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.

We divided each of THOR dimensions into several (3-4) topics – areas of interest. These topics are based on Consortium expertise, previous 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.

The CAMINO roadmap structure with dependencies between THOR dimensions, topics, objectives, milestones and actions is presented in the Figure 1.

Each topic addressed in our roadmap is presented in a unified way (in a full version if roadmap entitled “Comprehensive roadmap (research agenda) for fight against cybercrime and cyber terrorism”, ISBN: 978-83-64539-01-5, And in CAMINO deliverable D4.4)) 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.
- 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.
Figure 1: CAMINO roadmap structure
TECHNICAL ACTIVITIES OVERVIEW

#1 - Strengthening emerging tools - big data analysis and cloud security/forensics

Cyber attacks may not be visible on a small scale due to their nature or intensity (e.g. amount of traffic they introduce). Therefore, recently the techniques for using big data tools are being adapted. The recent research shows that 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 - establishing metrics and framework for cyber security testing

The IT world is becoming more dynamic, distributed and heterogeneous. This evolution implies novel security challenges, especially for security assurance. New methods for authentication, authorisation and trust management must deal with lack of pre-defined trust assignments and be ready to establish new relations with immediate effect. 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 incidents should be shared. The shared information can be used to get the correct assessment of security within 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 demanding aspects in every product, system or organisation is quality; guaranteeing fundamental characteristics such as reliability or availability in any system, moreover if it is a security one, it is an essential part of revealing the confidence of the development team in their system and/or product. Therefore, activities focused on maintaining and improving this quality are needed and the most effective ones are testing and simulation processes. Concepts such as automated tools or cyber exercises between companies will help to raise the awareness of not only people responsible for cyber security but also of the rest of the staff. And finally, in order to promote and encourage the realisation of these necessary actions, proper regulations and standards should be written and discussed, thereby achieving a desirable and prepared environment to benefit all these good practices.

#4- Countering cybercrime - botnets, Advanced Persistent Threats and cybercrimes affecting mobile devices and social networks

Nowadays, one of the main challenges affecting the fight against cybercrime is considerable with an increasing amount of evolving malware samples. Evolution and changeability of malwares and botnets (e.g. new, fast-evolving botnet architectures) are also factors that should be addressed by the research communities to more effectively fight against cybercrime. This is particularly important in the context of limitations of existing signature-based scanners and malware detectors. On the other hand, cybercrime also affects 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 the IoT (Internet of Things) concept.

**HUMAN ACTIVITIES OVERVIEW**

**#1 - Development of training tools and raising cyber security awareness**

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 users and those involved are properly kept abreast of the nature of the threat and the underlying rationale of the defensive steps being taken to mitigate it.

Whilst almost all new legislative changes are accompanied by training and situational awareness 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 - Promoting use of Privacy Enhancing Technologies**

With surveillance powers and techniques a very current topic, both from perceived excessive use in some quarters and 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 its regulatory interpretation.

In particular, DPR, eIDAS, and Payment Services Directive 2’s early adoption through SecuRe Pay, introduces requirements for the adoption of PETs, albeit through the adoption of undetermined techniques or technologies and 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. Regulatory requirements to assist consumers in remaining anonymous, for example with merchants online must also be seen in the light of requirements passed under the 4th Anti-Money Laundering Directive, which entered into force on the 26th June 2015, and which Member States have two years to enact.

**#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 for 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.
ORGANISATIONAL ACTIVITIES OVERVIEW

#1 - Adapting organisations to the cross-border nature of the Internet and cybercrime

Nowadays, competitiveness is global, so any company may receive an attack from anywhere on the planet. Therefore, most importantly, regulatory differences between countries should be understood and organisations should be aware of this fact and accordingly protect their assets and intellectual property. Therefore, organisations need to think “cross-border” regarding cybercrime and protect their networks globally.

#2 - Introducing cyber security as a society culture need

The use of new technologies is now not only present in the office, at home and at professional level but also during free time for children and adults and also to interact with the public sector, with banks, supermarkets and online stores. Moreover, these different functions overlap and initiatives such as BYOD are becoming more popular every year, mixing personal with professional activities. Therefore, cyber security is now crucial in terms of securing all aspects of day-to-day functions and should be introduced as a new culture capability.

#3 - Promoting EU institutional support to generic challenges and obstacles at the SME level

A common and unified institutional support is needed to promote changes at enterprise, company and SME level. The creation of an expert committee at the request of interested countries could contribute to overcoming these obstacles and challenges at a European level. In addition, an information sharing platform would support the approach and collaboration of interested parties prompting easier sharing of efficient ideas and problems. This support will assure the minimum protection needed in these matters.

#4 - Promoting EU cyber insurance market development

It is widely accepted that achieving perfect security is impossible. Security incidents and data breaches will occur regardless of the security controls and practices applied (though with much lower frequency). Thus, organisations have to deal with the residual risk. Recently, insurance, a common approach for residual risk, was applied to the cyber world. The developing cyber insurance market faces a number of unique challenges such as “heavy information” asymmetry, lack of statistical data, interconnected security and correlated risks, rapid change of risk landscape and unclear underwriting language etc.

The market in the USA is becoming increasingly mature with $2,75 billion in premiums for 2015 whereas the EU market is considerably less at $150 million for 2014 albeit increasing at the rate of 50% to 100% per annum. There are a number of steps which can be taken in order to help the EU market to flourish. The enforcement of a data breach notification law (which has currently passed the first reading in the European Parliament) will boost the EU cyber insurance market as the 2003 California bill did in the USA. Furthermore, information sharing on incidents, their consequences and prerequisites will help insurers get reliable statistical evidence. More advanced economical and regulatory models, together with technological advancements, will help reduce the effect of risk correlation. Last, but not least, scientific
studies are required to assess possible behaviour within the market place and identify incentives for individual organisations to increase their security level as well as the overall social benefit.

**REGULATORY ACTIVITIES OVERVIEW**

#1 - Investigatory powers in intra-jurisdictional and trans-border cases

Steps must be taken to instigate adequate investigatory powers as well as their use by LEA’s members regarding cyber-enquiries. The pace of regulatory reforms, the balance between abstraction and establishment of investigatory powers and the need for a training policy need to be taken into consideration. The effectiveness of international cooperation in trans-border cases, paramount to successfully prosecuting cybercrime, may be augmented in 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 risk to Fundamental Rights, one of the keystones of European culture. Efforts must be made in order to find a regulatory and technical framework allowing the juggling of augmented data exchange capabilities and respect of Fundamental Rights.

The regulatory driver towards greater levels of security in the face of cybercrime, such as promotion of more secure end-to-end encryption services and more advanced malware analytics, is being actively promoted by emerging EU Regulations.

One notable example, both of the regulatory move towards more coherent policy, but equally of some of the pitfalls faced, is the general Data Protection Regulation (DPR). The headline grabbing threats of penalties of up to 4% of global turnover combined with a first attempt at global enforcement have caused a great deal of concentration of minds on the need for organisations to protect their customer’s Personally Identifiable Information (PII), the contents of which are of interest to cybercriminals such as log in details and payment card information.

The DPR replaces the wide range of somewhat divergent nationally transposed Data Protection Act implementations stemming from the pre-existing Data Protection Directive. These national interpretations have led to a sometimes confusing array of data standards being applied across the 28 member states, with occasional attempts by the Commission to bring individual interpretations into line.

In principle these differences should be removed through harmonising Regulations rather than Directives. However, the permission of ‘exemptions’ from the DPR in cases of ‘national strategic interest’ is a potential source for ongoing differences in treatment across the European Union. One exemption that has the potential to cause ongoing confusion, and indeed friction, between Member States is in the lengths to which Member States are permitted to ‘infringe’ on the Data Protection rights of their citizens/subjects.

Interception powers and prohibitions vary from Member State to Member State, ranging across the spectrum of the privacy versus national security debate. The DPR’s drafting clearly sits more at ease with the view that privacy is paramount. However, the Member State with the highest adoption of e-
commerce, and hence key area of attraction from cybercriminal perspective, is the United Kingdom, where the Investigatory Powers Bill is in advanced stages of development. Whilst not commenting on the technical nature of such requirements, the parliamentary committee has agreed with the government's intention to seek access to protected communications and data when required if supported by a warrant, but not in requiring encryption keys to be compromised or system backdoors to be implemented. These ‘lawful intercept’ requirements, common in many nations, yet anathema to others, could become the source of tensions in the managing of ‘exemptions’ under DPR where cybercrime is noted as being required as an exemption in the national interest.

#2 - Civil and criminal courts forensics, admissibility and evidential standards

At present, there exists a wide variety of standards and best practices for information security and digital evidence gathering, amongst which the following ones can be emphasised:

- “Cobit, Framework for IT Governance and Control”, Information Systems Audit and Control Association, ISACA
- “Forensics sound techniques in the collection and analysis of digital and multimedia evidence “, Scientific Working Group Electronic Evidence
- “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice

This variety hinders the adoption of common standards and procedures for a strong foundation of cooperation and an effective fight against cybercrime and cyber terrorism at Pan-European level. This type of crime is particularly decentralised and not restricted to any frontier. The admissibility of digital evidence 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 a common understanding by adapting 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 maintained as a basic and key principle.

#3 - Electronic identity and trust services for data protection across borders

A majority of classes and applications of cybercrime and cyber terrorism contain a misrepresentation of identity or attempt to authenticate for access to goods or services to which the attacker has no legitimate use.
There currently exist a plethora of standards to identify and authenticate a genuine user as to who he or she claims to be and their access rights in the given circumstances. At present there is no interoperability with poor controls over the degree as to what constitutes ‘strong authentication’ sufficient for each application. However, within the European Union, the eIDentity, Authentication & Signatures Regulation, launched in October 2014 seeks to address these issues. Our CAMINO Roadmap will take account the timetable for its implementation and the external steps necessary to ensure international promotion.

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, was thought to show how quickly cybercrime and the standards to address it move. Yet by the final ratification in October 2015, just two months later, the SecuRePay minimum requirements for multi-factor authentication had been augmented with an additional requirement for dynamic linkages between the payer, payee, and transaction, a major additional security step to further secure against man-in-the-browser attacks.

Standards development is underway in both levels of assurance for eIDAS classification, and, whilst member states start transposition of strong authentication into national legislation the European Banking Authority has carried out (to February 2016) a Request for Information on cyber security standards, expected to lead to a formal consultation during the summer.

Meanwhile the striking down by the European Court of Justice in October 2015 of the Safe Harbour arrangements with the United States, where the storage of EU citizen’s data in the US, or access of such data by the US, was deemed compatible with EU requirements has led to a re-examination of the standards of trust in data sharing across borders. Following the Schrems case a re-evaluation of transatlantic data sharing was initiated, with the potential threat (and in some jurisdictions probably still threatened) that companies using US based servers or services were in strict breach of the ECJ ruling on minimum data protection requirements.
ROADMAP SUMMARY

The summary of roadmap activities for each THOR dimension and timeline (short-medium-long) is presented in figures 2 - 5.

TECHNICAL Dimension

**Objectives**
- Strengthening emerging tools - big data analysis and cloud security/forensics
- Security assurance - establishing metrics and framework for cyber security testing
- Improving preparedness - security engineering and testing capabilities
- Countering cybercrime - botnets, Advanced Persistent Threats and cybercrimes affecting mobile devices and social networks

**Perform testing activities - focusing both on the newly developed security solutions, as well as on the evolution of malware and botnets**
- Plan the research agenda
- Define a common taxonomy related to the malware and botnets
- Understand the main challenges resulting from the modern malware and botnets characteristics
- Identify gaps in standards
- Perform analysis of valid standards
- Collect best practices
- Prepare and organize national and Pan-European demonstrations and cyber exercises
- Introduce first modelling and simulation tools in the most critical sectors
- Define the awareness programs
- Define training programs for the future professionals in pentesting / testing capabilities and for companies
- Define requirements for cyber security open testbed
- Improve national and European legislation forcing companies to share the information about security incidents
- Prioritise current technologies, promote, and develop novel solutions
- Define business model for Pan-European infrastructures for cyber Big Data analysis

**Develop new security solutions and techniques that are complementary to the existing**
- Introduce new security standards and establish/support trusted assurance verifier agencies
- Provide clear legal support for collection, storage and analysis of shared data
- Make the technologies available for implementation and supporting related communities
- Develop research program for project(s) aiming at industrial trials of developed solutions
- Incentivise transfer of knowledge and resources (data samples, testbeds, etc.) between research institutions and other interested partners

**Support the evolution and continuous adaptation of security (detection and remediation) solutions to be more effective in the fight against malware and botnets**
- Launch first cyber security testbeds
- Create certifications studies in pen-testing, testing capabilities
- Analyse and design modelling and simulation tools for the rest of the strategic sectors
- Develop modelling and simulation tools for part of the strategic sectors

**Continuously scale up the testing environments**
- Continuously improve and adapt existing security solutions
- Operationally implement the newly developed (or adapted) solutions and first results of the fight against cybercrime and cyber terrorism based on the malware and botnets use
- Achieve complete acceptance of standards
- Develop modelling and simulation tools for all the strategic sectors
- Make available open testbeds for testing cyber security
- Harmonise national laws on European level and extend the cooperation with other countries
- Integrate technologies into more complex solutions
- Sustain community and monitor engagement

---

Figure 2: 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
HUMAN Dimension

Create a Pan-European Forum
Set standards of safeguards acceptable to both LEAs and users
Incorporate privacy enhancing functions and capabilities in newly developed applications and services
Effectively promote the PETs and awareness about data minimization, anonymisation and encryption techniques among society (data owners)
Continuously assess the capabilities of PETs in relation to newly developed emerging technologies

Promote understanding of value of user data, and potential applications for gaining user control
Assess the pros and cons of the various PET techniques within each use case
Collect and outreach best practices
Include cyber security topics in educational (school) programmes (at all levels)
Define gaps in cyber security protocols and standards
Define cyber security simulations and exercises at sectorial level
Define cyber security training at sectorial level
Continuously update awareness programmes and policies at an appropriate level

Attempt to internationalise agreed standards
Develop new encryption protocols for communication with privacy preservation
Adopt guidance on the appropriate use of PET, in each use case, within regulations and industry standards

Implement Cyber Security Information Sharing Partnership
Adopt the subject of cyber security as part of Master Degrees of Mathematics, Information Technology and Telecommunications
Continuously update and verify gaps in cyber security protocols and standards
Perform certifications and continuous updating. Perform simulations and cyber exercises at organisational levels
Develop cyber security training at organisational levels
Ensure, in mid-term, all cyber security experts, civil and military and decision makers are skilled in cyber security

Objectives
- Development of training tools and raising cyber security awareness
- Promoting use of Privacy Enhancing Technologies
- Appropriate use and re-use of data
- Adopt (on a greater scale) specialised Master Degrees in Cyber Security across all Member States
- Continuously update and identify gaps in cyber security protocols and standards
- Train cyber volunteers, from the public and private sector, who in case of cyber attack, would act under unified military command or CERT

Figure 3: 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
This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607406
REGULATORY Dimension

- Reinforce the cooperation channels regarding the fight against money laundering, especially concerning the financing of terrorism
- Strongly invest in fortifying the European data exchange system against unauthorised access and data theft
- Prevent an inconsequential implementation of any BD approach to the exchange of data concerning criminal cases
- Substantially reinforce the number and resources of cyber-enquiry-specialised police units and judiciary
- Determine the basic knowledge to be mastered by investigators in order to effectively use existing investigatory powers concerning cybercrime and IT investigation
- Reunite the EU and national actors concerned by the need for constant renewal of the investigatory measures

US EMV roll out
PSD2 early adoption through SecuRePay
eIDAS voluntary timeframe
Perform forensic awareness activities, in particular through appropriate education and training of the law enforcement and justice community
Establish minimum competence criteria for forensic science personnel
Include and provide safeguard of protection data issues in all EU funded research in digital forensics in H2020
Make a study of the applicable legislation at National and EU
Identify optimal and shared ways to create, update and use digital forensic databases at European level
Establish common best practice manuals and their application in daily work of forensic laboratories and institutes

Expected PSD2 mandate
eIDAS mandate
Accredit forensic science institutes and laboratories
Assess major challenges in the protection of citizens’ rights within the fight against cybercrime and cyber terrorism
Apply minimum quality standards for scene-of-crime investigations and digital evidence management from crime scene to court room
Implement digital forensics in the creation of the European Forensic Science Area
Recognise equivalence of law enforcement forensic activities
Establish automated means of international information sharing in virtual money transactions, allowing world-wide traceability of suspicious capital transactions
Promote full reciprocity in international cooperation for cybercrime prosecution on the basis of the wider consensus thus reached
If implemented, find a sufficiently restrictive regulatory framework
Launch basic formation programs on IT investigation and cybercrime all over the EU, directed to all investigators
Establish a permanent discussion platform in order to constantly assess the convenience of any update of investigatory powers relating to IT investigation and cybercrime

Objectives
- Investigatory powers in intra-jurisdictional and trans-border cases
- Civil and criminal courts forensics, admissibility and evidential standards
- Electronic identity and trust services for data protection across borders
- Conduct of proficiency tests and collaborative exercises in forensic science activities at International level
- Develop a comprehensive evolution of EU legal framework for data protection to address issues related to forensics and evidence admissibility
- Support homogeneous evolution of the Codes of criminal procedures of Member States to include systematic digital evidence admissibility
- Create European forensics principles and evidence admissibility agreements for the collaboration with external countries
- Maintain and improve the formation programs; include cybercrime and IT investigation as prerequisite for the access to the judiciary and the Police
- Consolidate and maintain the discussion platform

Figure 5: 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
CONCLUSIONS AND PLANS FOR THE ROADMAP EVOLUTION

In this document, we have presented the cyber security research agenda (the CAMINO roadmap) specifying our suggestions relating to future efforts in fighting against cybercrime 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 which is the basis for this roadmap, as well as for other research activities performed during the project.

Each of the four THOR dimensions described in the roadmap follow the same structure. Firstly, the top priority areas (topics) in the THOR dimensions have been defined. In summary, there are 14 key topics in the CAMINO roadmap. 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, ransomware 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.

The policy of Project CAMINO was to ensure wide consensus and agreement on the CAMINO roadmap encapsulating suggestions from relevant experts and stakeholder groups. The CAMINO Roadmap has been validated with feedback from experts as part of the evolution of the research agenda. In particular challenges relating to big data analysis, cloud forensics and to the cross-border nature of the use of the internet by cybercrime and cyber terrorism were evaluated as the most important and urgent problems to be solved.

In addition, we spent effort to avoid the situation where various means to counter cyber threats might be seen as individual “silos” or “islands” rather than a coordinated and joined up approach where all parties talk with each other. Therefore, some top level ideas include:
• Effective solutions, procedures and regulations for the police and LEAs (e.g. what types of cybercrime should be investigated and by whom, what means/techniques are allowed and could be used as evidence in the courts etc.).

• Effective solutions, procedures and regulations for prosecution – we need well trained prosecutors and well defined procedures for collecting and evaluating evidence.

• Effective solutions, procedures and regulations for courts and judges to clearly state what types of evidence can be admitted by courts to avoid the situation where the courts do not understand the cases.

• Effective solutions, procedures and regulations for trans-border cooperation and information sharing.

These are just some examples of the required improvements and actions to form an effective and comprehensive system. In particular, such a system should address the current needs and challenges that facilitate requirements for improvements to legal systems and related processes that impact upon all phases of cybercrime cases. One of the main efforts to be done is the improvement of digital forensic products, services and procedures. It is important to ensure an adequate flow of information at different stages of any investigation - from disclosure of crime, securing and preserving evidence and its processing, up to the judicial decision. In this context, it is also important to ensure and develop appropriate levels of knowledge and expertise across all the actors involved in the judicial process. Major improvement in information sharing and cooperation between victims, LEAs (the Police), the prosecution and forensic experts and finally the judges and courts is needed.

The CAMINO comprehensive roadmap can be now used by national funding agencies, by the EC to structure future calls by ENISA, EDA, etc. It can and is also used by national bodies working on national doctrines and strategies (such as 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 important feature of our approach is the comprehensiveness of the roadmap, since we believe that only holistic solutions can really help counter cybercrime and cyber terrorism.
CAMINO Consortium

ITTI Sp. z o.o.

CBRNE Ltd.

Consiglio Nazionale delle Ricerche

Data Fusion Research Center AG

Espion Ltd.

Everis Aeroespacial y Defensa S.L.

Montpellier University

Police Academy in Szczytno

S21sec Information Security Labs S.L.

Sec-Control Finland Ltd.