Comprehensive Approach to cyber roadmap coordination and development

How to improve resilience against cybercrime and cyberterrorism?

prof. Michal Choras, DSc, PhD Eng
FP7 CAMINO Coordinator
ITTI Sp. z o.o.
London, 15th June, 2015
Agenda

• Cybersecurity experience
• FP7 CAMINO project
  – Consortium
  – CAMINO THOR approach
  – Cyber crime and cyber terrorism – current problems
  – CAMINO roadmap – topics
  – CAMINO regulatory dimension
  – CAMINO workshops
  – Cyber think-tank
• Conclusions
ITTI – key facts

• SME – ca. 50 employees with professional certificates, e.g. PRINCE2, ITIL, BS 7799/ISO 27001, TOGAF 8, Certificate in Software Testing (SJSI/ISTQB)

• Prizes and rewards (selected):
  • „Cristal Brussels Prize 2006, 2010 and 2013” for the most active and successful Polish SME participating in EU 6 and 7 Framework Programme
  • reward for the high performance in R&D projects for European Defence Agency

• Membership in international bodies:
  • Public Safety Communications Europe (PSCE)
  • Integrated Mission Group for Security (IMG-S)
Cybersecurity – research projects

FP7 Security projects:
- FP7 INSPIRE/INSPIRE-INCO
- FP7 INTERSECTION
- FP7 CAMINO (Coordinator)

EDA/NATO projects:
- EDA ATHENA
- NIAG studies

Active participation:
- Integrated Mission Group – Security (IMG-S TA7)
  Thematic Area Cyber Security (vice-chair: Michał Choraś)

DG Home
- CIPHER

National projects:
- SOPAS
- SECOR

CAMINO – key facts

Main strategic objectives:

1) To develop a comprehensive cyber crime and cyber terrorism research agenda,
2) To initiate long term activities providing a stable platform of security research experts and organizations.

- Acronym CAMINO: Comprehensive Approach to cyber roadMap coordINation and develOpment
- Topic 2.5-1 of FP7-SEC-2013-1
- ITTI Sp. z o.o. coordinates the project
- 10 Consortium members
- 8 countries
- 21 Supporting members
- Duration: 24 months (1 Apr 2014 – 31 Mar 2016)
- Total cost of the project: 1,036 M€
CAMINO Consortium

1. ITTI Sp. z o.o.
2. CBRNE Ltd.
3. Consiglio Nazionale delle Ricerche
4. Data Fusion Research Center AG
5. Espion
6. EADE
7. Montpellier 1 University
8. Police Academy in Szczytno
9. S21SEC LAB
10. Sec-Control Finland
Multidimensional nature of cyber security

CAMINO THOR Approach

• **Technical** – both offline and online aspects of cyber security

• **Human** - various human and societal contexts beyond the core technology

• **Organizational** - policies, roles, responsibilities in relation to cyber security

• **Regulatory** – legal status of cyber security
Cyber security – current problems (1/2)

• Technical examples:
  – Fighting against growing and evolving malware and botnet
  – 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 of Things
  – New methods for Authentication and Authorization
  – Information sharing platforms or mechanisms and Dynamic Risks Assessments
  – Mobile devices protection
  – APTs protection
  – Insider threats detection and Protection
Cyber security – current problems (2/2)

• Human and ethical aspects:
  – Training, awareness, and management/monitoring/mitigation
  – Individual rights vs. societal rights
  – Privacy

• Organizational:
  – The Challenge of the Global Nature of the Internet
  – Challenges due to the nature of Cyber-Crime
  – Challenges and obstacles at the Enterprise/Firm Level

• Regulatory:
  – Common regulations and differences in legal systems
  – Technical language and cyber definitions in law
  – Slow evolution of law
CAMINO roadmap topics

Dimensions (THOR)

CAMINO Roadmap

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

Human
- Development of Training and Awareness tools

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

Regulatory
- Investigatory Powers in intra-jurisdictional & trans-border cases

Topics

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

Introducing Cyber security as a society culture need

Interoperability of Common and Roman Law

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

Civil and Criminal Courts forensics/admissibility/evidential standards

Raising the cyber security awareness

Comprehensive system to fight against cyber crime/cyber terrorism

Comprehensive Approach to cyber roadmap coordination and development

D4.3 – CAMINO Roadmap (research agenda) – first version
CAMINO roadmap topics

Technical topics
• Strengthening/Adapting emerging tools - Big Data analysis and cloud security/forensics
• Countering Cyber Crime - botnets, Advanced Persistent Threats and cyber crimes affecting mobile devices and social networks
• Security assurance - improvements in authentication and authorisation, trust management and information sharing
• Improving preparedness - security engineering and testing capabilities

Human topics
• Development of Training and Awareness tools
• Utilising Privacy Enhancing Technologies
• Appropriate use and re-use of Data
CAMINO roadmap topics

Organisational topics
• Adapting organisations to the cross-border nature of the Internet and Cybercrime/Terrorism
• Introducing Cyber security as a society culture need
• Promoting EU Institutional support to Generic Challenges and Obstacles at the Enterprise/Company/SME Level

Regulatory topics
• Investigatory Powers in intra-jurisdictional & trans-border cases
• Interoperability of Common and Roman Law
• Civil and Criminal Courts forensics/admissibility/evidential standards
• Identity/Authentication Standards for Data Protection across borders
CAMINO Roadmap – cross-dimension topics

- Raising the cyber security awareness (including Human and Organizational dimensions)
- Comprehensive system to fight against cyber crime and cyber terrorism (including all THOR dimensions)
CAMINO roadmap – regulatory dimension: topics and objectives

• Investigatory Powers in intra-jurisdictional & trans-border cases
  – Reducing the gap between the average efficacy of investigations in “real-world” enquiries and cyber-enquiries by adequate investigatory powers
  – Finding an effective, Fundamental rights-compliant framework for the future of data exchange between national and EU law enforcement authorities
  – Improving the efficacy of the investigatory powers beyond the EU borders (cybercrime and money laundering)

• Interoperability of Common and Roman Law
  – Speed/need for adaptation of law for offences committed using new technology/techniques
  – Relative ‘ease of use’ in intra-jurisdictional dispute resolution
  – Civil and Criminal Courts forensics/admissibility/evidential standards
CAMINO roadmap – regulatory dimension: topics and objectives

• To reach homogeneity and European consensus of the admissible forensic analysis process for digital evidence
  – To specifically adapt and update the current legislation to the cyber and digital scenario
  – To coordinate the future evolution of citizens’ rights protection with the adoption of new evidential standards

• Digital forensics training and certification schemes
  – Identity/Authentication Standards for Data Protection across borders
  – Agree levels of Authentication
  – Align public/private eIDAS levels within EU
  – Manage interoperability internationally
Regulatory dimension: summary of actions

Objective 1: Investigatory Powers in intra-jurisdictional & trans-border cases

- Reunite the EU and national actors concerned by the need of constant renewal of the investigatory measures (EU and national regulators and LEAs, magistrates, hardware and software developers, Academia)
- Determine the basic set of knowledge to be mastered by investigators (policemen, magistrates) in order to effectively use existing investigatory powers concerning cybercrime and IT investigation
- Substantially reinforce the number and resources of cyber-enquiry-specialised police units and magistrates
- Prevent an inconsequential implementation of any BD approach to the exchange of data concerning criminal cases
- Strongly invest in fortifying the European data exchange system against unauthorized access and data theft
- Foster the renegotiation of reciprocity in the Budapest Convention on cybercrime fighting
- Reinforce the cooperation channels regarding the fight against money laundering, especially concerning the financing of terrorism

- Establish a permanent discussion platform in order to constantly assess the convenience of any update of investigatory powers related to IT investigation and cybercrime
- Launch basic formation programs on IT investigation and cybercrime all over the EU, directed to all investigators (not only to those specialised or more likely to directly cope with cybercrime)
- Reach a point of equilibrium
- If implemented, find a sufficiently restrictive regulatory framework
- Promote full reciprocity in the international cooperation for cybercrime prosecution on the basis of the wider consensus thus reached
- Establish automated means of international information sharing in virtual money transactions, allowing world-wide traceability of suspicious capital fluxes

Consolidate and maintain the discussion platform
Maintain and improve the formation programs; include cybercrime and IT investigation knowledge as prerequisite for the access to the Magistracy and the Police
Regulatory dimension: summary of actions

In line with development of wider legal and transnational investigation legislation

Objective 2: Interoperability of Common and Roman Law
- Establish common best practice manuals and their application in daily work of forensic laboratories and institutes
- Make a study of the applicable legislation at National and EU level to detect the issues which collide with current and expected future digital scenarios, and to identify existing gaps
- Include and provide safeguard of protection data issues in all EU funded research in digital forensics in H2020
- Establish minimum competence criteria for forensic science personnel
- Perform forensic awareness activities, in particular through appropriate education and training of the law enforcement and justice community
- Identify optimal and shared ways to create, update and use digital forensic databases at European level

Objective 3: Civil and Criminal Courts forensics/admissibility/evidential standards
- Recognise equivalence of law enforcement forensic activities
- Implement digital forensics in the creation of the European Forensic Science Area
- Apply minimum quality standards for scene-of-crime investigations and digital evidence management from crime scene to court room
- Assess major challenges in the protection of citizens rights within the fight against cyber crime and cyber terrorism
- Accredit forensic science institutes and laboratories

Objective 4: Identity/Authentication Standards for Data Protection across borders
- Create European forensics principles and evidence admissibility agreements for the collaboration with external countries
- Support homogeneous evolution of the Codes of criminal procedures of Member States to include systematic digital evidences admissibility
- Develop a comprehensive evolution of EU legal framework for data protection to address issues related to forensics and evidence admissibility
- Conduct of proficiency tests / collaborative exercises in forensic science activities at international level

Known timelines:
- eIDAS voluntary timeframe
- PSD2 early adoption through SecuRe Pay
- US EMV roll out
- Expected PSD2 mandate
- eIDAS mandate
## CAMINO workshops

[http://www.fp7-camino.eu/events](http://www.fp7-camino.eu/events)

<table>
<thead>
<tr>
<th>EVENT</th>
<th>PLACE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st CAMINO workshop</strong></td>
<td>Bern, Switzerland</td>
<td>September 18th, 2014</td>
</tr>
<tr>
<td><strong>2nd CAMINO workshop at Mobile World Congress</strong></td>
<td>Barcelona, Spain</td>
<td>March 3(^{rd}), 2015</td>
</tr>
<tr>
<td><strong>CAMINO-COURAGE workshop</strong></td>
<td>Montpellier, France</td>
<td>April 8(^{th})-9(^{th}), 2015</td>
</tr>
<tr>
<td><strong>3rd CAMINO workshop</strong></td>
<td>London, England</td>
<td>June 15(^{th})-16(^{th}), 2015</td>
</tr>
<tr>
<td><strong>Final CAMINO workshop</strong></td>
<td>Madrid, Spain</td>
<td>March 2016</td>
</tr>
</tbody>
</table>
CAMINO Think-Tank

- **Informal initiative** – an association of loosely coupled experts, i.e. does not have any legal status and is not formally registered, e.g. as a non-profit organization.
- **The main objective** - exchange of experience and knowledge and dissemination of information related to the effective fight against cyber crime and cyber terrorism to the wide audience.
- Taking into account variety of dimensions related to the fighting against cyber crime/terrorism – from technical and legal to human and organizational aspects impacting countering of cyber crime and cyber terrorism.
- Declaration of participation is available at:
  http://www.fp7-camino.eu/camino_think_tank
- **We kindly invite You to join and participate!**
Thank you for your attention

Contact:
Prof. Michal Choras (ITTI Sp. z o.o.): michal.choras@itti.com.pl

www.fp7-camino.eu