Consolidated Research Roadmap

Cagliari, May 2016

Ben Brewster

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research
Sheffield Hallam University

http://www.courage-project.eu
Contents

• Context and Overview
• COURAGE Approach
• COURAGE / CAMINO Consolidation
• Towards the consolidation of the CyberRoad Outputs
• Sustainability - CyberConnector
Consolidated Research Roadmap

- Convergence of three projects funded under FP7 security call 2013.2.5-1 aiming to define research agendas focused on cybercrime and cyberterrorism.
Context

• In response to recommendations made at the joint first review meeting of the CAMINO, COURAGE and CyberROAD projects, held at the offices of the European Commission, Brussels on June 4th 2015

• The three consortia have undertaken to consolidate each of their respective outputs into a single, unified and easily digestible research roadmap that can be distilled to inform future works, related policies and funding initiatives that address the challenges being faced by society due to the proliferation of cybercrime and the threat of cyberterrorism.

• Here we present an initial draft of these topics across four interlinked dimensions Technical, Human, Organisational and Regulatory.

• The topics highlight a number of what we collectively consider to be priorities for future research and practice. We do not consider these topics to be comprehensive, but a reflection of the themes and subject areas that featured most prominently across the three projects.
COURAGE Approach

- Develop a Cyber Crime and Cyber Terrorism (CC/CT) research agenda for the European Commission to significantly improve the security of citizens and critical infrastructures, and to support crime investigators towards enhancing
- This Research Agenda will identify the major challenges, reveal research gaps, and will identify and recommend detailed practical research approaches to address these gaps through strategies that are aligned to real-world needs.
The COURAGE approach builds on three pillars,

• A user centric methodology, to identify gaps, challenges and barriers based on real-world needs and experiences;
  – Through consultation with more than 75 domain stakeholders and experts using a wideband 'Delphi' approach to unpack the tangible 'wants and needs' of society

• An analytical and semantic approach, to deliver a taxonomy and create a common understanding of the subject with all stakeholders; and
  – Through a comprehensive analysis of existing initiatives and research.

• A competitive and market oriented approach, to foster practical implementations of counter-measures using effective test and validation solutions.
  – To identify tangible means to assess the impact and quality of activities occurring as a result of the research agenda and roadmap.
Requirement Elicitation Process
This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.

**Thematic distribution and Representation**

- **Government**: 6%
- **Academic**: 32%
- **Law Enforcement**: 28%
- **Private Sector Security**: 28%
- **Judicial**: 3%
- **Public Sector Security**: 3%

**Themes**

- Cross Border Regulation and Jurisdiction
- Resource Provision (training, funding etc.)
- Human Rights, Citizen Protection and right to privacy
- Anonymity Issues
- Data (large volumes / Big Data)
- Investigators Capacity / Capability / training
- Defining (distinguishing and understanding)
- Awareness / Education
- Technological Evolution
- International & Public/Private Collaboration (inc. info sharing)
- Legal systems/frameworks inc. Data Protection / Privacy Issues

**Topics**

- Human Rights, Citizen Protection and right to privacy
- Anonymity Issues
- Data (large volumes / Big Data)
- Investigators Capacity / Capability / training
- Defining (distinguishing and understanding)
- Awareness / Education
- Technological Evolution
- International & Public/Private Collaboration (inc. info sharing)
- Legal systems/frameworks inc. Data Protection / Privacy Issues
This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.

COURAGE Data

Total Distribution of Topics by Thematic Group

- Technological Issues: 27%
- Law and Policy: 28%
- Awareness Education and Training: 16%
- Cooperation & Info Sharing: 15%
- Definitional Issues: 7%
- Specific Threats: 4%
- Other: 3%

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.
Consolidation with Camino

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

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949
### Consolidation with Camino

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

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.
Human Dimension: Awareness, Education and Training

• Focused on increasing awareness and education levels at all levels

• From ‘grass roots’ initiatives and national teaching curricula, right through to improving the availability and access to specialist skills in Law Enforcement and the private sector.

• Considered a key mitigation vector for a broad array of vulnerabilities

• Importance only likely to increase given the way in which ‘cyber’ continues to extend traditional forms of criminality.

• Cited as important dimension across different stakeholder groups, and by agencies such as ENISA and Europol in annual threat assessments.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.
Organisational Dimension: Cross border Issues

- Cybercrime a truly ‘borderless’ phenomenon
- Created an environment where we are increasingly reliant on mechanisms that facilitate cooperation:
  - Between international authorities (i.e. across borders)
  - And the public and private sectors
- Key requirement to incentivise ‘voluntary and proactive’ cooperation at both levels.
- Analysis of existing mechanisms for effective practices and barriers (MLAT etc.)
- Supporting the work of EC3
- Both within and (especially) beyond boundaries of the EU
### Workshop Results: Urgency

#### Urgency of Research Items

<table>
<thead>
<tr>
<th>Research Item</th>
<th>Low</th>
<th>Med</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive legal system to fight against CC/CT</td>
<td>10%</td>
<td>62%</td>
<td>28%</td>
</tr>
<tr>
<td>Electronic identity and trust services for data protection across borders</td>
<td>5%</td>
<td>67%</td>
<td>28%</td>
</tr>
<tr>
<td>Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction</td>
<td>8%</td>
<td>64%</td>
<td>28%</td>
</tr>
<tr>
<td>Promoting EU institutional support to generic challenges and obstacles at the enterprise/company/SME level including incentives for cyber insurance</td>
<td>23%</td>
<td>44%</td>
<td>33%</td>
</tr>
<tr>
<td>Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges</td>
<td>21%</td>
<td>51%</td>
<td>28%</td>
</tr>
<tr>
<td>Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism</td>
<td>8%</td>
<td>31%</td>
<td>62%</td>
</tr>
<tr>
<td>Definition, characteristics and behaviours of the offenders and victims in cybercrime</td>
<td>21%</td>
<td>56%</td>
<td>23%</td>
</tr>
<tr>
<td>New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies</td>
<td>13%</td>
<td>56%</td>
<td>31%</td>
</tr>
<tr>
<td>Collective awareness and education for increased societal resilience to CC/CT threats</td>
<td>5%</td>
<td>46%</td>
<td>49%</td>
</tr>
<tr>
<td>Countering cybercrime affecting mobile and IoT devices</td>
<td>10%</td>
<td>30%</td>
<td>60%</td>
</tr>
<tr>
<td>Establishing metrics and frameworks for cyber security testing</td>
<td>8%</td>
<td>53%</td>
<td>40%</td>
</tr>
<tr>
<td>Strengthening emerging tools for big data analysis, cloud forensics and security</td>
<td>8%</td>
<td>53%</td>
<td>40%</td>
</tr>
</tbody>
</table>
Workshop Results: Necessity

Prioritization of Research Items

- Comprehensive legal system to fight against CC/CT: 40%
- Electronic identity and trust services for data protection across borders: 41%
- Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction: 44%
- Promoting EU institutional support to generic challenges and obstacles at the enterprise/company/SME level including incentives for cyber insurance: 44%
- Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges: 44%
- Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism: 44%
- Definition, characteristics and behaviours of the offenders and victims in cybercrime: 36%
- New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies: 38%
- Collective awareness and education for increased societal resilience to CC/CT threats: 38%
- Countering cybercrime affecting mobile and IoT devices: 38%
- Establishing metrics and frameworks for cyber security testing: 35%
- Strengthening emerging tools for big data analysis, cloud forensics and security: 35%

Legend: Low, Medium, High

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949
Towards Consolidation with CyberRoad

Anti-malware Research

Authentication and Anonymization (cybercrime attribution)

Behavioural security and NO-PWD systems

Cryptography and Public-Key Infrastructures

Cybercrime and the Economy

Computer Forensics

Healthcare Systems

SCADA & CIP

Information Exchange

Law & Order

Networking

Cyber Threat Awareness

New objects and ‘disappearing computing’

Social Resilience

SDCL & Architectures

Threat intelligence and Attack Detection

Trust chain & identity

Vulnerability Assessment

<table>
<thead>
<tr>
<th>Regulatory</th>
<th>Organizational</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybercrime and the Economy</td>
<td>Critical Infrastructure Protection</td>
<td>Authentication and Anonymization: Cybercrime Attribution</td>
</tr>
</tbody>
</table>

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949
## Towards Consolidation with CyberRoad

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Technical</th>
<th>Human</th>
<th>Organizational</th>
<th>Regulatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topics</td>
<td>[T1] Strengthening emerging tools for big data analysis and cloud forensics and security</td>
<td>[H1] Collective awareness and education for increased societal resilience to CC/CT threats</td>
<td>[O1] Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism</td>
<td>[R1] Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction</td>
</tr>
<tr>
<td></td>
<td>[T2] Establishing metrics and framework for cyber security testing</td>
<td>[H2] New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies</td>
<td>[O2] Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges</td>
<td>[R2] Electronic identity and trust services for data protection across borders</td>
</tr>
<tr>
<td></td>
<td>[T3] Countering cyber crime affecting mobile and IoT devices</td>
<td>[H3] Definition, characteristics and behaviours of the offenders and victims in cybercrime</td>
<td>[O3] Promoting EU Institutional support to generic challenges and obstacles at the enterprise/company/SME level including incentives for cyber insurance</td>
<td>[R3] Comprehensive legal system to fight against CC/CT</td>
</tr>
</tbody>
</table>

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949.
• Again, brings together the outputs of COURAGE, CyberRoad and CAMINO.
• In total, 16 chapters divided into four sections.
  • I: Approaching cybercrime / cyberterrorism research
  • II: Legal, ethical and privacy concerns
  • III: Technologies, scenarios and best practices
  • IV: Policy development and roadmaps for cybercrime / cyberterrorism research
• Will be available in time for the final project reviews in June 2016
Sustainability through CyberConnector

COLLECTIVE KNOWLEDGE BASE TO IMPROVE CYBER-SECURITY
CROSS-CUTTING KNOWLEDGE, SKILLS AND CAPABILITY NEEDED TO UNDERPIN ALL OUR CYBER SECURITY OBJECTIVES

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607949
• CyberConnector is an online space open to private organisations, public administrations, CERTs, law-enforcement agencies and individuals to create, enhance and collective knowledge to improve cyber-security.

• Hosting different communities focusing on the fight against botnets, cyber-risks assessment, social vulnerability assessments and more, CyberConnector hosts communities focusing on the detection and mitigation of botnets, assessing cyber-risks, identifying needs in fighting cyber-terrorism and on-going collaborative European projects.
To Join, visit [CyberConnector.eu](http://CyberConnector.eu) and click ‘Ask-for-an-Account’