Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Law and Order

Author(s): Lizzie Coles-Kemp (RHUL), Rogerio Bravo (PJ), Angelo Consoli (SUPSI)

CC RG-92– Training of law enforcement officers and legal authorities on laws relating to the new paradigm. Development of new laws and research on strengthening of old laws dealing with online cybercrime and cyber terrorism.
CC/CT LEG-6 – Research to better understand how to extend the EU legal framework in response to cybercrime and, at the same time, preserve the privacy of the citizen.
CT RG-92 – Research to better understand infrastructures on the Internet that support underground flow exchange of using online means.

ABSTRACT

The gaps identified by the social, economic political and legal research stream within Cyber ROAD are categorised within two clusters: social resilience and law and order. The following gaps have been prioritised for research action because they are representative of the three law and order main themes to emerge from the Cyber ROAD analysis. These three themes are: development of an integrated and well-coordinated global approach to fight cybercrime and cyber terrorism, privacy-aware tools and legal frameworks for cybercrime fighting and enhanced identification of internet-enabled money laundering practices at both the social and data network levels.

The research to develop an integrated and well-coordinated global approach to fight cybercrime and cyber terrorism is focused on the training of law enforcement officers and legal authorities to respond to cybercrime and cyber terrorism and the development of new laws and research on strengthening of old laws responding to cybercrime and cyber terrorism.

The research to develop an improved legal framework research explores the practicalities of developing and deploying a European cybercrime fighting framework. The research gap also examines the practicalities of remote access, develops improved methods of remote access to digitally stored evidence and analyses the tensions between individual privacy and the data access needs of the crime fighting agencies.

The research to enhance identification of internet-enabled money laundering examines the topic from both the social and data network perspectives and enhances the understanding of how money laundering is manifested on the internet and the social and technical infrastructures used to support internet-enabled money laundering.

RESEARCH ACTION #1

Developing an enhanced, integrated global response from crime fighting agencies
The research action is focused on developing an enhanced, integrated global response from crime fighting agencies to cybercrime and cyber terrorism.

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **2 STREPs and 1IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **Law enforcement agencies, academics, law makers, government**

This research action addresses the following research questions:

- What education programme is most effective in training law enforcement officers in responding to cybercrime and cyber terrorism?
- What is the structure and contents of the legal paradigm needed to respond to cybercrime and cyber terrorism?
- What are the effective means of communicating the new legal paradigm to law makers?

A research programme is needed to co-ordinate existing expertise and develop effective methods of communicating the new legal paradigm to law makers so that prompt, effective legislation change becomes possible in every legal jurisdiction. This research action aims to develop an integrated and well-coordinated global approach to fight against cybercrime and cyberterrorism. It is focused on the training of law enforcement officers and legal authorities on laws relating to cybercrime and cyber terrorism, the development of new laws and research on strengthening of old laws dealing with online cybercrime and cyber terrorism. One of the main outputs of this research will be a new legal paradigm for responding to cybercrime and cyber terrorism. Research is necessary to determine the most effective way of teaching law enforcement officers so that their expertise in responding to terrestrial crime can be transformed into new expertise in responding to cybercrime.

Research is necessary to identify the new laws necessary to respond to cybercrime. In particular, research is needed to build a picture of the new legal paradigm necessary to respond to cybercrime and cyber terrorism, examine where the new legal paradigm converges and diverges from the current legal paradigm and identify gaps in legislation that is necessary to respond to cybercrime and cyber terrorism. As part of the design of the new legal paradigm, the conceptualization of legal jurisdiction will need to be examined.
This research action comprises the following stages:

1. Review of current legal paradigm and gap analysis of capabilities in the context of cybercrime and cyber terrorism.
2. Stakeholder consultation as input to the design of new legal paradigm
3. Public policy updates and proposals

Enhancement of the European Legal Framework

This research action explores how the European Legal Framework might be enhanced to better respond to cybercrime and at the same time preserve the privacy of the EU citizen.

DISTANCE TO THE MARKET: **TRL 1**
COST OF THE TOPIC: **2 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **Crime fighting agencies, governments and law makers**

The research questions that this research action addresses are:

- What constitutes an effective cross-border data sharing framework for cybercrime fighting that preserves the privacy of the citizen?
- How can effective remote access to digital data stores for cybercrime evidence gathering be facilitated?
- How can the relationships between digital evidence data stores best be visualized in order to support cybercrime fighting?

This research action seeks to extend and standardise the legal framework in order to enable the crime fighting agencies to more rapidly investigate cybercrime.
An enhanced legal framework needs to have the following capabilities:

a) communicate privacy issues to the public;
b) visualise the relationships between data stores that contain the evidence necessary for a cybercrime investigation;
c) provide effective remote access to digital data stores for evidence; and d) safeguard privacy and human rights when accessing digital data stores for cybercrime investigation

There is strong motivation for such a programme - without their being clear legal consequences for cybercrime, the perceived chance of being identified or brought to justice is small. At the same time, EU citizens use cryptography to protect their personal data on social media platforms that use data storage outside of the EU. This means that the EU does not have sovereignty over the critical data necessary to deter, prevent, investigate and prosecute criminals. This also means that the EU has to redefine traffic data as a legal concept that moves beyond simply identifying the IP address and to make the content of this traffic available to law enforcement agencies during an investigation.
This research action comprises the following stages:

1. Review of the existing framework for digital evidence access and identification of gaps in capability.
2. In partnership with the stakeholder communities, design of revised frameworks of digital evidence access and identification of privacy tensions for citizens.
3. Development, deployment and assessment of tools and methods to support the legal framework and to respond to the identified privacy tensions.

RESEARCH ACTION #3

Study practices and processes of internet money laundering
This research action examines infrastructures that support internet enabled money laundering.

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **1 STREP**
AVAILABILITY OF COMPETENCE IN EUROPE: **2**
TIME SPAN FOR ADDRESSING THE ACTION: **24 months**
ACTORS: **Academics, industry and government, consumer and citizen representatives**

This research action addresses the following research questions:

- What are the most effective ways to study the flow of internet-based money laundering transactions?
- What internet infrastructures support money laundering?
- In what ways has the Internet influenced money laundering practices?

This research action aims to derive a better understanding of how the internet has influenced the nature of money laundering. In particular, this research action will look at how money laundering transactions flow across the internet. This research will also explore how the internet has resulted in changes to money laundering practices. The research will further develop our understanding of the internet infrastructures that are currently used in money laundering and how these might evolve in the future.

The research action will bring together both social and computational science researchers. The social research will focus on the historical practices of money laundering and examine how these have been influenced by the use of the Internet for money laundering. The social research will also examine to what extent the use of the internet has affected the take-up of money laundering services, the roles of money laundering within crime networks and the ability of traditional interventions to disrupt money laundering activities. The computational research will examine how money laundering transactions can be identified on the data network, the transaction patterns generated by internet-enabled money laundering and the traceability of the transaction patterns.

This research action would comprise the following stages:

1. Survey of existing academic and practitioner literature on money laundering practices.
2. Field research to identify the impact of the Internet on money laundering practices and the communities that both carry out and consume money laundering services.
3. Lab research to examine how money laundering transactions manifest themselves on the data network.
4. Development, deployment and assessment of new techniques to identify and trace internet-enabled money laundering.