Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda

Borka Jerman-Blažič, Tomaž Klobručar
Laboratory for Open Systems and Networks
Jožef Stefan Institute
Ljubljana, Slovenia
{borka, toma@e5.ijs.si}

Abstract—Cybercrime and cyberterrorism remain important problems of today’s society. Insufficient resources for the fight against cybercrime and cyberterrorism require research activities in this field to be allocated where the gaps exist. This paper presents results of the COURAGE project process to identify missing research items in the area of cybercrime and cyberterrorism. In total, 12 main issues that need further research are identified and described in detail. The results that are part of the COURAGE research agenda are important for various stakeholders, such as researchers, industry, policy makers, and law enforcement agencies.

Keywords—cybercrime; cyberterrorism; research item; research agenda; research gap; COURAGE project

I. INTRODUCTION

Cybercrime (CC) and cyberterrorism (CT) remain important problems of today’s society. Not only that the fight against CC/CT is lagging behind, current cybercrime attacks are becoming more aggressive and confrontational [1]. As resources for the fight against CC/CT are limited in most of the EU countries, it is essential that they are allocated to the areas where gaps exist and where the potential results have the highest impact. A research agenda for developing and deploying the missing solution could contribute to the more effective efforts in developing solutions for prevention of or fight against CC and CT by identifying research challenges, revealing research gaps, and identifying and recommending the research activities to address those gaps.

The two-year COURAGE (Cybercrime and Cyberterrorism European Research Agenda) project (http://www.courage-project.eu) from the EU Seventh Framework Programme was selected to deliver a comprehensive research agenda and the aligned roadmap. 17 organisation from 12 European countries collaborated together with the main stakeholders in the field. The final project results were delivered in May 2016. This paper presents briefly the main research agenda items and identifies missing solutions that require further deployment.

The paper is organized as follows. In Section II, we describe the applied methodology for identification and evaluation of the research agenda items. Section III describes 12 most important research items classified in the research agenda, while conclusions are given in Section IV.

II. METHODOLOGY

The identification and validation of the research agenda items was run through several steps as follows.

A. Workshops with Stakeholders

The stakeholder requirements were collected during seven thematic workshops with 32 participants, the first one was a pilot workshop followed by six workshops dedicated to specific domains (critical infrastructure, technology, law ethics) or target groups (academia, government, law enforcement). In total, 31 requirements were identified during the workshops, classified into 6 themes: enhancing the capability of investigators; cooperation and information exchange; organisational and societal resilience; legislative systems and data protection; awareness, education and training; and technological evolution.

B. Research Gap Analysis

In parallel to the workshops, a gap analysis in the relevant fields was performed. It was based on the COURAGE taxonomical categorisation of CC/CT and the inventory of past and on-going research activities identified through the EU projects with topics addressing cybercrime and cyberterrorism, the literature databases, and other information sources such as Europol, ENISA, UNICRI, OECD, or ITU.

The gaps were grouped according to the main topics of the COURAGE CC/CT taxonomy. The topics include offences against the confidentiality, integrity and availability of computer systems, computer related offences, content-related offences, or offences related to copyright infringement, as well as actors and their motivation and their practices, and CC/CT prevention measures. In total, 47 research gaps were identified.

Each of the identified gaps was considered as a candidate for a research item and equipped with the attributes that describe: how easy/likely the gap is to be filled; the estimated time that the gap would be filled if it were given resources and attention by the community; a level of gap abstraction; and comments that offer necessary context for the gap. The template for research items description was adapted from the CAPITAL project [2].
C. Evaluation of Candidate Research Items

The stakeholder requirements and identified research gaps were prioritised based on abstraction (strategic over technical), achievability, and timeline, and cross validated to create a single candidate for the CC/CT research items list. The final results of this procedure were 13 research topics equipped by the specific challenge description, scope, and expected impact.

D. Validation workshop

Finally, the list of research items was evaluated during a workshop with 8 experts from different disciplines who updated, refined, reshaped and consolidated their descriptions. After the workshop two similar items on cooperation with the private sector were joined together which resulted into the final list of 12 research items.

III. RESEARCH AGENDA ITEMS

This section reviews the main research items that were identified and validated by the described methodology.

A. Legitimacy and Effectiveness of Blocking Illegal Content

The primary aim of content blocking online is to prevent users from receiving or accessing specifically targeted illegal content from servers hosted in different countries. Two primary approaches to dealing with the challenge of managing illegal online content are removal of unlawful content at the source or provider side and blocking access to unlawful content at the destination or user side.

The specific challenges are related to the differences in national laws and policies between countries involved, in particular regarding human rights and fundamental freedoms, and the legality of content. Content stored on servers within a certain country, for example, may not be deemed illegal, but it would be illegal in the country receiving/accessing it. Similarly, human rights and fundamental freedoms, e.g. freedom of speech and freedom to receive information, are valued more in one country than another.

The scope of these challenges requires a balance to be achieved between protecting potential victims and the integrity of human rights principles. This topic poses the requirement for research that focuses on assessing legal systems, governance, policies and data protection regulations for evaluating the effectiveness of blocking illegal content. In particular, different legal frameworks affecting cross-border evidence gathering and the use of geo-location technology are suggested as two important areas of consideration.

B. Preventing and Countering Hate Speech and Content-related Offences that Support Terrorism

In recent years, the Internet has become a widely used medium by extremists, terrorists and hate groups in order to spread fear, hatred and violence [3]. The shift to social media has resulted in a new approach in terrorists’ communication practices, with engagement in psychological warfare, propaganda distribution and the indoctrination or radicalisation of “lone wolf” terrorists being the most pressing issues [4, 5].

The main identified challenges in this area are lack of officially recognized definitions of hate crime and hate speech and inconsistent legal response between EU countries [6], shortage of reliable data on the issue, and poor awareness of how to respond to the issue. Effective solutions to prevent/counter fear and hate speech/violence spread via the Internet are needed. Research should explore the radicalization and the origins and evolution of the origin and the motivation of the terrorist and extremist groups. Ineffectiveness and counterproductive approaches of Internet blocking and monitoring technologies to disrupt and monitor terrorist and extremist communications [7, 8] also call for research for development of alternative or additional measures such as the use of counter-narratives, taking into account the difficulties and legal constraints of such action. Similarly, research involving profiling and monitoring of users of extremist sites would be of great value in terms of providing a high level overview to support policy interventions. Legal and ethical implications of the use of profiling should be included, as well as practical difficulties.

C. Detection and Prevention of Computer-related Fraud

The specific challenge here is to achieve a better understanding of detection methods in relation to user and system behaviour as well as discovering anomalies and certain deceitful characteristics. Speed of response to fraudulent actions is key to preventing or minimising damage and loss, therefore methods for early detection and sustained response requires to be explored. A particular focus on policies, regulation and educational methods in relation to software vulnerabilities is also emphasised as additional item for research.

In general, it is identified that research is required focusing on raising awareness and developing training across all sectors of the society. Awareness includes understanding victims’ point of view, and understanding why individuals and organisations often do not report being victims. Research should identify better ways for law enforcement agencies and vulnerable sectors, such as the financial sector, to work together for combating and preventing fraud. Best practices for countering social engineering and phishing should also be explored.

D. Understanding Challenges to the Securitisation of Copyright and Enhancing the Effectiveness of Detection and Prevention Methods

Online copyright infringement is a complex area of cybercrime, due to the wide range of perpetrators and victims involved and the different levels of offending. Competing interests and diverse approaches to dealing with this problem add to this complexity. Equally strong and opposing arguments are made in relation to the general criminalisation of copyright infringement and the protection of net neutrality and freedom of information.

Research is needed to evaluate the existence of new methods of categorising, prioritising and dealing with the disparate cases of copyright infringement, potentially offering alternative best practices to those currently deployed. Research
should work alongside legal and ethical bodies to determine a 'sliding scale' of severity of crime, as there is currently a lack of pan-European discourse. On an international level, research is needed to establish a common understanding in relation to commercial scale copyright infringement and those involved with it; both suppliers and consumers. Research is also required that will provide improved awareness and training for those tackling and dealing with this type of cybercrime, including the legal, political and investigation sectors.

E. Definition, Characteristics and Behaviour of the Offenders and Victims in Cybercrime Events

The scale of Internet use as a means to facilitate crime has introduced a need for more thorough analysis of cyber-criminal and victim profiles, and identifying the intent and motivation behind the attacks. Despite the importance of analysing the various different actors, there has been little progress to date. One of the reasons for the current gap in research in this area is the lack of understanding of the physical and virtual areas where cybercrime and cyberterrorism take place and the lack of information about offenders and victims. Relevant data sources and appropriate methods of collection need to be found to fill in information gaps. Of particular importance is learning about victim and offender profiles in respect of criminal adaptation and exploitation of technologies.

Particular attention also needs to be paid to 'insider threats' which may deliberately or accidentally impact upon businesses, organisation, services and infrastructure. Given the importance of aims and motives of actors in distinguishing between cybercrime and cyberterrorism, there is also a need for further understanding of the human factors that lead to attacks of each type. The effectiveness of current criminal-psychological investigations into extremism and radicalization should be evaluated as well.

F. Advanced Tools for Digital Investigation in Compliance with the Privacy Legislation and Regulation

The specific challenge which faces investigators is to achieve a balance between fundamental human rights in relation to data protection and privacy and effective law enforcement techniques necessary to tackle CC/CT.

Higher capabilities of the tools used by the investigators to collect and analyse large amounts of (potentially personal) data are needed, whilst at the same time they have to adhere to various data protection laws in different European countries and underlying fundamental human rights. The scope of future research should be focused on the development of methods and techniques for data acquisition and analysis so that effective CC/CT investigations can be carried out without infringing on fundamental human rights and national and European laws and agreements. This would include employing technologies which protect privacy at each stage of data processing. The role of privacy enhancing technologies and transparency enhancing technologies in facilitation of the big data analysis without breaching data protection and human rights laws need to be investigated and developed further. It is essential to develop effective techniques which also adhere to robust EU privacy standards and serve to reassure the public.

G. Preventing and Countering CC/CT Activities on the Dark Web and Similar Networks

Part of the Internet known as the Dark Web or Darknet is inaccessible for traditional investigative tools and technologies and has recently come to global attention as one of the environments for the preparation and implementation of illegal activities aimed at both physical and virtual environments. Whilst the Dark Web was neither created nor intended for illegal purposes, it does allow access to illegal markets, covert meeting places and criminal databases. It makes use of applications and network protocols for encryption and anonymization that hinder law enforcement in discovering and investigating illegal activity. There is a need for the development of a full toolset (technical, managerial and legal) for law enforcement agencies that can help in identifying offenders and prevention of their illegal activities. Research in this field should address topics, such as marketplace analysis, coordinated international action to perform covert investigations on the Dark Web, coordinated international action to counter and limit the abuse of anonymity on privacy networks like Tor and I2P, and tools for locating and mapping hidden service directories and tracing attackers and criminals.

H. Definition and Harmonisation of Terms in CC/CT throughout the EU

The definitions used in reference to cybercrime and cyberterrorism are, in some instances, inconsistent across EU Member States, potentially causing confusion and hindering law enforcement, prosecution and international cooperation efforts due to the lack of a common understanding of terms. Harmonisation of terminology in cybercrime and cyberterrorism is thus crucial in facilitating LEA cooperation in a European and broader, international context. This research priority is related to defining and harmonising the terminology used in the area of cybercrime and cyberterrorism so that the elements that make up the offences and the way they relate to each other can be categorised and commonly understood. Clear, unambiguous and universally understood terms and definitions of cybercrime are necessary to enable those measuring, predicting, combating, investigating and prosecuting such crimes, to do so effectively. It is important that the definitions incorporate different aspects and themes of cybercrime and cyberterrorism, so that their interrelations and various contexts can be categorised and classified. Definitions based on a comprehensive taxonomy will also enable metadata specification and standardisation.

I. Standardisation of Methods for Enhancing Preventative Tools and Strategies Pertaining to CC/CT

The availability and adoption of appropriate standards can play an important role in driving improvements in establishing practices for auditing, risk assessments and assuring information security, not only from a technical but also a broader, organisational perspective. Furthermore, increased inter-dependencies across the wider supply chain further reinforce the requirement for the adoption of harmonised standards and a common language for managing cyber-security risks. The activities are needed to create an understanding of the ways in which preventing and responding to cybercrime
can benefit from using refined standard methods for cybersecurity.

J. Dealing with Different Levels of Legal Frameworks for Illegal Content: Questions of Geolocation and Jurisdiction

Cyber-attacks can involve a large number of different countries and jurisdictions whereby a cyber-criminal is located in one country, assessing and controlling computers based in different countries and affecting victims in third countries. In the absence of harmonised international and national legal frameworks applying to this type of challenged, this ‘internationalisation’ of crime makes the reporting and deletion of illegal content, as well as the collection of court evidence and court testimony, very complicated. In addition, the absence of physical proof and the frequent anonymity of perpetrators complicate the task of LEAs in collecting admissible evidence. Research should investigate how to deal with lack of physical proof and cross-jurisdictional cases (e.g. examine the opportunity of introducing a dispute settlement procedure for illegal content cases). Research should also explore the possibilities and limitations of geolocation technologies in containing and fighting the dissemination of illegal content on, or with the aid of, the Internet.

K. International and Public/private Cooperation

The fight against CC/CT requires strong cooperation between national authorities, as well as between public and private sectors. Such cooperation is not easy, given the differences in languages, culture, and resources, lack of incentives for the private sector to share information, etc. Future research should develop improved methods and best practice guidelines for formal and informal collaboration between the Internet industry and state agencies and clarify the roles of the different actors involved, particularly in regulating content. Laws, regulations and policies that may provide obstacles to cooperation should also be identified, and strategies determined so that these can be overcome. Legislation needs to clearly define responsibilities, limitation of powers and the extent of human rights in respect of privacy and data protection, in the context of investigatory procedures. A balance must be achieved between the interests of investigating crime, thereby ensuring public safety, and citizens’ rights of privacy and data protection.

L. Collective Awareness and Education for Increased Societal Resilience to CC/CT Threats

Increasing awareness and standards related to online safety and information security play an important role in improving societal resilience to cybercrime [1]. Moreover, ‘human’ security is acknowledged to be important factor as popular attack vectors such as social engineering and phishing continue to exploit human security vulnerabilities [9]. Research should focus on the identification of new approaches to increasing societal awareness, and subsequently readiness, to deal with cybersecurity threats. Where necessary, the impact of new and emerging technologies and behavioural changes that occur because of them should be identified and considered. The research should identify and address awareness and education requirements across levels and sectors, such as national teaching curricula, law enforcement and other public and private sector institutions. Alongside an evaluation of existing approaches, all stakeholders should be engaged, from cybersecurity experts, to citizens, to policy makers and the private sector, to establish means to proactively target the awareness and education requirements of users.

IV. CONCLUSION

Research agendas are an important instrument for prioritizing future research activities. In this paper 12 items that need further research are described for the domain of cybercrime and cyberterrorism. The items are part of the COURAGE research agenda that outlines in addition the recommended short, mid and longer term actions for each of the described research items and the roles of different stakeholders (law enforcement agencies, solution providers, research and technology organisations, policy makers, legal, ethical and societal stakeholders, accreditation and certification bodies, and educational institutions) in the actions [10].

ACKNOWLEDGMENT

This work has been supported by the European Commission through the COURAGE (Cybercrime and Cyberterrorism European Research Agenda) project from the Seventh Framework Programme. The contribution of the COURAGE partners is acknowledged.

REFERENCES


[10] B. Brewster et al., Final research agenda, including the roadmap of recommendations for a system of horizon scanning of new CC/CT threats, COURAGE D5.6 deliverable, May 2016.