COURAGE

CYBERCRIME and CYBERTERRORISM EUROPEAN RESEARCH AGENDA

Our Vision for the Future of Research in Support of the Fight Against Cybercrime and Cyberterrorism Research

COURAGE is funded under the European Commission's 7th Framework Programme for research, technological development and demonstration under grant agreement number 607949, FP7-SEC-2013.2.5-1.2

Beginning in April 2014, the COURAGE (Cybercrime and cyberterrOrism (E)Uropean Research AGEnda) project undertook to deliver a research an agenda in order to define and inform the priorities for future cybercrime and cyberterrorism research. Funded under the EU's FP7 programme the agenda identifies major challenges; reveals research gaps and recommends practical research approaches to address these gaps through strategies that are aligned to the real-world requirements of practitioners, policy makers, citizens and other stakeholder groups. These strategies are supported by test and evaluation schemes defining metrics and performance indicators used to assess the impact of actions taken as a result of the project's research roadmap. COURAGE's work was undertaken with the overall objective of defining practical, grounded approaches that will assist in supporting business and critical infrastructures, the capability of crime investigators and enhancing the security of European society as a whole.

To achieve this, COURAGE has undertaken to address a broad range of key challenges, such as the speed and implications of technological change, raising awareness and education levels, the transnational scope and nature of cybercrime, data protection, cooperation and information sharing issues, amongst others. In this final report, we present a high level overview of the topics, trends and priorities identified throughout the project, as a public artefact that articulates many of the key project findings delivered by the project to the European Commission at the projects conclusion in April 2016.

Contents

COURAGE Research Items

Priorities for research related to cybercrime and cyberterrorism

Introduction

In order to establish the research items contained within this report, the project adopted a wideband Delphi approach[1] as its primary means of electing and prioritising topics for research from the extensive network of stakeholders associated with the project. In total, more than seventy different stakeholders, representing law enforcement, academia, critical infrastructure, the telecoms industry, security professionals, and other bodies were consulted. The approach, consisting of four main rounds; an initial survey acting as a boundary setting exercise, followed by three rounds of focus groups, was used to bring together opinions from a broad range of stakeholder groups in order to identify key contemporary challenges faced by domain practitioners, researchers and other stakeholders. These findings were then subsequently cross-validated, using a literature survey that analysed existing works and initiatives targeted at these areas trying to identify where gaps remained. Based upon the findings from this process we present the following research topics. They provide insight into a number of areas where, we believe, there is scope for research to make a significant impact in enhancing society's overall resilience to threats emerging from the cybercrime and cyberterrorism landscape.

Research Topics

Improving the legitimacy and effectiveness of blocking illegal content (including governance, regulatory and criminal procedures)

Blocking illegal content, on the whole, currently consists of two main approaches; removing it through notice and takedown procedures at the source or provider side and applying filtering and blocking techniques to prevent access at the destination or user side. The specific challenges that arise from these actions are associated with the difference in various nations' laws and policies, particularly in relation to human rights and data protection. Illegal content incidents typically affect more than one country, and therefore will be defined and dealt with differently according to the nation's approach to illegal content and human rights. There needs to be a balance achieved between these different approaches so that cybercrime occurring across several jurisdictions can be dealt with more effectively. Research under this topic should evaluate different legal systems' effectiveness in blocking illegal content and how different laws affect cross-border evidence gathering and the potential application of technology in determining geo-location. However, it is often difficult to identify offenders in order to bring them to justice; therefore research should address ways of overcoming this challenge. Transparency is also an important aspect to be addressed under this topic. Efficient methods for achieving transparency may assist in providing more clarity about what content is blocked and why.

Preventing and countering hate speech and other content-related offences that support terrorism

Work carried out by high-level European institutions and organisations such as Europol and the Council of Europe, has identified the extensive use of the internet by extremists, terrorists and hate groups to spread fear and violence, including psychological warfare, distribution of propaganda and indoctrination of 'lone wolf' terrorists. It has been shown to be particularly effective in furthering the cause of such groups and has resulted in exposing many people, particularly those considered to be most vulnerable in society, to such content. Response to these activities poses a number of challenges including those associated with deficiencies in definitional and legal consistency, and a shortage of reliable data and uncertainty in how to respond most effectively. Effective ways to prevent and counter illegal content are needed, as some actions have been shown to be ineffective and counterproductive, for example providing a list of blocked sites which can be reverse-engineered. Human considerations associated with both offenders and audiences should also be addressed by research proposals. It is important to understand the characteristics and behaviours of offenders, but also of targeted audiences. Research which uses profiling and monitoring of users of extremist sites might be of great value, although the legal, social and ethical implications of this kind of research would need to be considered extremely carefully.

1 For an overview of the Delphi approach see Dalkey, N.C. (1969). The Delphi Method. http://www.rand.org/pubs/research_memoranda/RM5888.html

Improving the detection and prevention of computer-related fraud

Computer-related fraud can be defined as an act of deceit to gain an unfair advantage through illegal access to, or interference with, a computer system. Typical acts include deception to obtain economic benefit, evading liability or the creation of false data as a result of interfering with a computer system. Preventing or minimising damage and loss are the main objectives of those dealing with computer fraud and therefore methods for early detection, particularly in relation to user and system behaviour, anomalies and deceitful characteristics, as well as sustained response need to be further explored. Although laws exist to deal with this type of offence they are ineffective unless offences are noticed and reported. Victims are often oblivious to their details being stolen or are reluctant to report incidents. Research which adopts victims' point of view and explores reasons for lack of reporting would enable a clearer picture of the nature and extent of fraud to be revealed. In turn, research could also be carried out which focuses on awareness raising and training. With this foundation, computer fraud detection methods for private users could be developed. Working together to combat fraud is another key area; research proposals should identify better ways for law enforcement agencies (LEAs) and vulnerable/targeted sectors to collaborate. With new methods of committing fraud being developed all the time, it is essential that current and emerging threat types are included in research proposals which would support continued education, training and awareness and enable a more effective response to be developed.

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 the 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. Many difficulties largely stem from the fact that copyright infringement is a general term for a wide range of actions; from accidental, unintentional or negligent small-scale actions to the large-scale activities that undermine industries and are viewed as a threat to economies. There is a need for research to define categories of offences based on generally agreed upon criteria, taking into account different types of impact (e.g. social, economic) and providing, in collaboration with legal and ethical bodies, a sliding scale of severity of crime which can then be understood and dealt with appropriately. Large-scale copyright infringement should be researched at an international level to create a common understanding and to further enable cooperation internationally between all key stakeholders. There is also a need for research to provide knowledge about different types of offenders and their methods in order to provide increased awareness and training for those tackling this form of cybercrime.

Definition, characteristics and behaviour of the offenders and victims in cybercrime events

The scale and proliferation of internet use as a means to facilitate crime has also introduced new challenges for the social and behavioural sciences in addition to the technological and criminological disciplines we normally associate with studies in the domain. Due to the potential overlaps and absences of clarity in distinguishing between cybercrime, cyberterrorism, cyber warfare, and often the inability to identify the origin of an attack means that there is significant benefit in assessing the impact of an attack and discerning the potential motivations behind it. The significant and widespread impact exerted by modern cybercrime means that individuals and groups involved in committing, responding to, and, preventing events, is equally expansive. The sheer quantity and diversity of the criminal actors and victims of cybercrime means that despite the importance of analysing the various categories of actors, there has been little progress to date. In order to develop, deliver and improve intervention and prevention measures, this topic proposes research to help build our understanding of the diverse range of actors involved. Existing research has shown that cybercrime is no longer the preserve of technically skilled individuals and groups, so more work is needed to establish the underlying factors that contribute to the profiles of victims and offenders alike, in addition to establishing human, economic and other factors that drive cybercrime.

Advanced tools for digital investigation in compliance with data protection legislation and regulation

This research area acknowledges the competing challenges faced by law enforcement agencies in the investigation of cybercrime. There is a need to achieve a balance between privacy and data protection and effective law enforcement techniques necessary to tackle cybercrime. The nature of the offences often requires LEAs to collect and analyse large amounts of (sensitive) personal data. A number of recent high-profile incidents involving large internet providers, and government agencies have led to increased suspicion and mistrust by the public in relation to data collection by public authorities. Therefore, investigation tools, including computer forensics, which proactively respect privacy and data protection rights, need to be developed. This will serve to reassure the public and ensure investigations are compliant with legislation. The ways in which Privacy Enhancing Technologies and Transparency Enhancing Technologies can be used in an investigative context needs to be further investigated. Research should adopt a pan-

European approach and take into account recent legislative changes in the area of data protection. Reassurance and trust between digital service providers, data controllers and LEAs also needs to be increased. This would assist in creating mutual understanding and long lasting cooperation.

Preventing and countering CC/CT activities on the dark-web and similar networks

Part of the internet known as the 'Dark Web' has become infamous due to its use as a vector for the proliferation of a wide range of illegal activity. This is facilitated by the use of applications and network protocols for access, encryption and anonymisation making it largely inaccessible using traditional investigative tools and technologies. Many different types of crime, often including the most serious and organised, are supposed to be facilitated or carried out in this environment. In recent years, drug and weapon trafficking, terrorist activity and child sexual abuse among others have all been alleged to make use of 'dark-web' services. There are also indications that the dark-web is increasingly being used to host botnet command-and-control infrastructures. Research in this area needs to focus on the nature and behaviour of those engaging in illegal activity in this environment and the development of tools and technologies to discover and counter such activity. This would also help to create a manual of standards, norms and good practices for further research. Research under this topic can ensure maximum impact and exploitation of results by involving relevant end-users, such as law enforcement agencies.

Definition and harmonisation of CC/CT terminology throughout the EU

The definitions and understanding of terminology used in reference to cybercrime and cyberterrorism are, in some instances, inconsistent across EU Member States, potentially causing confusion, and in extreme cases, hindering the effectiveness of law enforcement, prosecution and international cooperation efforts due to the ambiguity surrounding the subject area in general. Harmonising terminology in cybercrime, cyberterrorism and criminal and terrorists use of the internet is crucially important in defining how the law enforcement sector should cooperate in an EU and broader international context. Without a clear understanding of the characteristics that distinguish them, these areas will be hard to addresses properly across all relevant levels. The absence of equal representation and understanding of terms from both areas of cybercrime and cyberterrorism, the lack of definition of terms and the different taxonomies in current use in the field have been identified as problems by academia, LEAs, and by entities representing legal and ethics organisations as well as from the critical infrastructure stakeholders. In this topic, it is proposed that efforts must be made to increase levels of knowledge exchange among stakeholders, leading to the provision of harmonised and standardised terms through the development of a new taxonomy framework that involves all aspects of cybercrime and cyberterrorism, specifying their differences and commonalities.

Standardisation of methods for enhancing preventative tools and strategies pertaining to CC/CT

Reliance on computerised information systems is an everyday feature throughout every sector of society. Despite this fact, cyber and information security are frequently considered to be IT problems, rather than appreciated as the wider organisational risk that it is. The adoption of appropriate standards can play an important part in establishing practices for auditing, risk assessments and assuring information security, not only from a technical but also a broader, organisational perspective. Such measures also serve to create harmonised standards and a common language for managing cyber-security risks across the wider business supply chain. Research should adapt existing approaches and propose new holistic ones. The benefits of responding to cybercrime can then be understood in the context of specific requirements of different sectors, of small to medium enterprises and of critical infrastructure. Road-mapping the pathways to this type of activities requires engagement with standardisation and other EU bodies so that challenges related to cybersecurity, cybercrime and cyberterrorism can be addressed consistently and comprehensively.

Managing different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction

Cybercrime is increasingly a cross-border issue, potentially involving a number of different countries and territories each with their own legal frameworks and jurisdictions. This 'internationalisation' of crime creates new challenges for law enforcement. It includes issues such as the reporting and deletion of illegal content, the collection of court evidence, cross-border accessibility of data and other issues. Related to the problem of gathering court-admissible evidence in this context, is the issue of locating offenders in order to bring a prosecution. Geolocation technology has been only partly successful in this respect and more research is required to understand and address the ability of cybercriminals to act anonymously. The location of criminal activity and the location of the victims also raises issues about investigating and prosecuting offences. In the absence of harmonised international and national legal frameworks, which country enforces laws and whether the online content is deemed illegal in all countries that it affects are important complications to be addressed. In this research topic, the identification and development of new methods that enable LEAs to gather and share information across geographic borders resulting in improved cross-border cooperation among international and public/private authorities is required, which will support the development

of new standards for harmonising collaboration between the private sector and law enforcement.

International and public/private cooperation

The importance of cooperation between national authorities and the various public and private sector organisations in the fight against cybercrime and cyberterrorism has been widely acknowledged. Tackling the complexity of such criminality is no longer the sole remit of law enforcement; but rather the responsibility and commitment of all those involved. In particular, the private sector is well positioned to carry out proactive tasks such as botnet takedowns and discovering and blocking online illegal content as well as providing technical support and specialist software to law enforcement. Although some positive steps have been taken to facilitate strong cooperation, holistic success is still some way off and encouraging cooperation and identifying practical ways to increase levels of information sharing between those involved remains a key area for research, policy makers and practitioners alike. Differences on many levels create challenges in this regard. Willingness to share data, different legal systems, language barriers, and cultural and policy differences are key difficulties. Another important issue is the perception of those involved with and affected by actions and more needs to be done to raise awareness in order to find a pathway through the uneven legal landscape and foster a culture of genuine cooperation. Frequently, the private sector is reluctant to share the personal data of their customers and there have been several instances where public opinion has opposed the introduction of measures that facilitate or mandate it. Thus, the requirement for a balance between ensuring public safety and the respect of what are seen as the fundamental rights of individuals is needed. Research focusing on specific issues within this area needs to explore current barriers to international and public / private cooperation so that the roles and limitations, in respect of legal restrictions and societal acceptance, are fully understood. Best practice guidelines, incorporating greater incentives and safeguards, can then be provided to achieve better collaboration and so increase cyber-resilience on an international scale.

Collective awareness and education for increased societal resilience to CC/CT threats

This topic focuses on the identification and facilitation of new approaches to enable the enhanced resilience of society to cybersecurity threats through increasing the awareness and education of groups and individuals across society. All categories and levels of stakeholders across society will have to be involved in order to make such an initiative truly successful, ranging from citizens through to security professionals, policy makers and the private sector, with special focus on critical infrastructure providers and operators. Prevention strategies, and in this context, particularly those associated with increasing awareness and standards related to online safety and information security, play an important role in improving societal resilience to cybercrime. At the same time 'human security' specifically is an import factor as popular attack vectors such as social engineering and phishing continue to exploit human security vulnerabilities. Under this topic, research will focus on the identification of new approaches to increasing societal awareness, and subsequently readiness, to deal with cybersecurity threats and cybercrime. Where necessary, the impact of new and emerging technologies and behavioural changes that occur because of them should be identified and considered. The research proposed should identify and address awareness and education needs across levels and sectors, such as national teaching curricula for citizens, training for law enforcement and other public and private sector institutions, evaluating the relative successes of existing initiatives in order to further refine our understanding of what is, and can be, successful in this context.

Road-mapping Future Research

Introduction

The COURAGE Research Roadmap (D5.5) provides a description of different stakeholder roles and an outline of recommended actions for each of the COURAGE research items described above. The roadmap proposes a number of short, mid, and longer term actions to enable the achievement of the expected impacts outlined within each of the research items. These recommended actions are presented across three primary target groups (law enforcement agencies (LEAs), solution providers, and research and technology organisations (RTOs)) and four areas of focus (legal, ethical and societal issues, policy, accreditation and certification, and education and awareness-raising). The following summary outlines the key actions suggested for road-mapping the implementation of the COURAGE research agenda across each of these categories. Although we will not go into specifics regarding the impact timeline in this report, we do include here a number of summaries which outline some, but not all, of the challenges and priority areas for research in respect of the aforementioned stakeholder groups and areas.

Roadmap Areas

Solution Providers

One of the primary recommended avenues for private sector collaboration is through working more directly with LEAs. This collaboration could lead to the development of new ways to detect and monitor illegal usage; to identify technologies that can be exploited to facilitate cross-border evidence acquisition and in bridging cross-border

jurisdictional and information sharing issues. Throughout the process of the project, a number of specific examples of areas have been identified where it is considered that solutions providers can contribute. These include: systems monitoring users and content associated with identified extremist groups; recognising hate speech and content related offences that support terrorism on the web and social media; tools to combat computer related fraud; tools to assist in the early detection of cyber threats and new vulnerabilities that can be exploited to breach the security of computer systems; tools to detect and prevent copyright infringement; automated data acquisition methods (including from the Dark Web and Darknets); and improving the interoperability of software systems.

Law Enforcement Agencies

LEAs across all EU Member States face new challenges, posed by the proliferation of new and emergent forms of criminality, particularly those further enabled by, and in some cases dependent on the penetration of the web and information systems into almost all facets of the public and private sectors and the everyday lives of citizens. The scope of online crimes such as fraud and identity theft has increased, while recent analyses have suggested trends towards more aggressive and overt forms of crime, with the use of extortion becoming commonplace via the use of crypto-lockers. Furthermore, cybercrime is no longer the sole remit of skilled, technically literate, or well-resourced criminal enterprises, since tools that enable DDOS and other attacks are becoming available to those with lower levels of computer savviness. The challenges faced by law enforcement are further-compounded by financial austerity measures, which have resulted in significant funding cuts across many European police forces.

For these reasons, the inclusion and involvement of LEAs serves two broad purposes: Firstly, in developing competitive advantage in terms of preventative and investigatory capability, and secondly, as a means of increasing efficiency in response to the aforementioned spending cuts. The actual value proposition of LEA involvement comes in the form of contributing information on actual trends in criminal behaviour, existing practices, and requirements for fighting crime. It is worth noting that there have been multiple signs of positive development and progression that can be built upon further. COURAGE stresses that such practices should be further reinforced alongside additional best practices and recommendations.

Research and Technology Organisations

RTOs play a vital role in the realising society's response to many of the threats associated with the continued challenges of cybercrime and the emerging threat of cyberterrorism. Academic institutions play two roles in this regard. Firstly in unpacking the theoretical and practical challenges identified in the domain towards enabling and facilitating the development of practical solutions, recommendations and contributing to society's wider knowledge pool. Secondly, academia is also responsible for educating the next generation of experts, and other professionals, and developing the teaching curriculum for future generations. RTOs can also play a part in Computer Emergency incident Response Teams (CERTs), and regularly lead the development of technological breakthroughs in security.

With respect to the solution providers, RTOs have a unique complementary position in being able to channel, test, and transfer innovation with a longer-term perspective. In cooperation with European authorities, they are also able to support the definition and proposal of policies by providing environments in which the potential impact of regulations can be tested. Indeed, one of the key cyber-related challenges we are facing builds on the fact that the traditional mechanisms of evolution, identification, prosecution are not applicable in practice. Firstly, because CC and CT propagate at speeds and through channels that we cannot easily oversee. Secondly, because it is inherently a cross border issue, thereby creating the need for a trans-national legal framework that is only just beginning to emerge. Finally, because it leaves a trail of electronic data and information the uptake and usage of which as a valid base in prosecutions are neither fully defined nor agreed upon. In this context, RTOs could play a key role both in deploying test beds for innovative approaches and in linking the interests and activities of the private sector and public authorities.

Legal, Ethical and Societal Stakeholders

European and national legislative authorities have an essential role to play in the areas of regulating the blocking of illegal content, defining the different scales of IP infringement, providing a constitutional balance between surveillance and privacy, as well as defining appropriate data retention obligations.

Recent events have only escalated the privacy vs. security argument among security stakeholders and commenters, re-emphasising a number of issues around the legal and ethical challenges associated with cyber-security. Part of this involves the legality (and ethics) associated with the use of encryption and anonymisation tools on the internet and legislation to support the protection of fundamental rights. Legal and ethical aspects require thorough research if adequate legislation is to evolve in these areas. This research includes looking in more depth at the responsibilities and liabilities of internet service providers and their interplay with prosecution and intelligence services. Specific areas identified for research include investigating further issues around the harmonisation of legislation across borders, content blocking standards, privacy and other fundamental rights and freedoms.

Policy Makers

From a policy perspective, the implementation of the research agenda should be mainly supported through mechanisms of collaboration between relevant EU and Member State agencies, and other key CC/CT stakeholders.

The following have been identified as areas where it is foreseen that policy actors can have an impact: supporting the pan-European implementation of research priorities, providing frameworks for collaboration between CC/CT stakeholders across borders, to promote standardisation efforts, and to encourage and support research funding. These efforts should be strengthened through the setup of a public-private partnership; the public side being led by the European Commission with support from Europol/EC3, and the private side being led by representative industry organisations.

Accreditation and Certification Bodies

Any certification and standardisation initiatives need to address specific challenges, motivators, incentives, and barriers and constraints, which should be taken into account when implementing the suggested research agenda items. There are a number of challenges associated with standards related to information/cyber-security. Firstly, there is a lack of clarity, guidance and in some cases incentive, available on what standards organisations should comply with in order to sufficiently meet their specific organisational needs. The following drivers are considered as important for future research: Legal and regulatory compliance, risk reduction or transfer, increasing the levels of security.

Awareness, Education and Training

I n terms of raising levels of awareness, and education and training related to the fight against cyber-securityCC/CT, it and the risks associated with cybercrime it is possible, and perhaps indeed necessary, to differentiate between a number of different groups and actors and their unique needs and requirements of them. At a grass-roots level, the education of end-users on web hygiene and internet safety through awareness initiatives and national teaching curricula is considered vitally important. Taking this requirement further, the education of the next generation of security experts through nurturing the talent pool at a university and post-graduate levels is also of extreme importance, as is process that will also assist in developing training curricula for levels of education across other professions, including law enforcement, the justice system, critical infrastructure protection and others.

Horizon Scanning for Future Threats

Introduction

The high speed of technological change and continued emergence of new threats are two of the main characteristics associated with the field of CC/CT. Prediction and prompt identification of new threats as well as the evaluation of future threat developments and the means to address them is thus crucial for the successful fight against CC/CT. The main goal of this section is to to provide guidelines for the continued horizon scanning of such threats, influenced primarily by the challenges highlighted in the project's research items and the wider challenges being faced by society in respect of CC/CT. The approach described includes recommendations for a horizon scanning methodology, data sources for horizon scanning, and criteria for the evaluation of threats. Horizon scanning has been defined as "the systematic examination of potential (future) problems, threats, opportunities and likely future developments, including those at the margins of current thinking and planning. Horizon scanning may explore novel and unexpected issues, as well as persistent problems, trends and weak signals" (Van Rij et al., 2010).

Horizon Scanning

When developing a system of horizon scanning COURAGE selected to adopt an integrated and inclusive approach. The integrated approach implies that horizon scanning is combined with the methods utilised as part of the research item and roadmap development approach, namely the wideband Delphi method, and the PESTLE and research gap analyses. The inclusive approach implies that horizon scanning combines both exploratory and issue-centred scanning as well as participatory and non-participatory methods (Amanatidou, 2012). Just as the environment changes over time, the process of horizon scanning is not a one-time exercise, but an ongoing process of analysis to evaluate new and emergent challenges (Van Rij et al., 2010). In order to achieve this, the following mechanisms are recommended.

The Delphi Method

COURAGE recommends a three stage approach to the identification and evaluation of threats, utilising open-ended questionnaires, themed expert workshops and focus groups, as has been demonstrated throughout the course of the project in defining priorities for future research aimed at unpacking the tangible requirements of society and its stakeholders.

Desk Based Research

Desk research, including the review of academic and practitioner literature from public databases, internet searches, and social media monitoring should be undertaken in order to keep up-to-date on current state-of-the-art research, initiatives and practice so that identified challenges remain relevant and build upon current and existing work.

Topic Focusing

The described methods are used for scanning of the following items:

Threats - Cybercrime and cyberterrorism offences and threats according to the COURAGE taxonomy, i.e. offences against the confidentiality, integrity and availability of

computer systems and networks, content-related offences, triggered incursion or offences related to intellectual property (including copyright) infringement and other fraudulent acts.

Technologies – existing and emerging technologies that might pose security threats in the future if these technologies are abused.

Domain specific threats – threats specific for certain CC/CT domains, such as critical infrastructure, Internet of things, Dark Web, payment systems, …

Specific COURAGE research agenda items related threats - including hate speech and content-related threats for terrorism support; computer related fraud threats; copyright infringement threats; new types of offenders or new behaviours and practices of the offenders; anonymous communication.

Evaluating the Significance of New Threats

Four criteria are used to assess potential threats: severity of the threat, likelihood of its realisation, impact on the society, and threat maturity. They are described briefly in the following section.

Severity of a threat
Severity of the consequences on the society in case of the realisation of the threat:

- High (H): Threat realisation would cause major damage to the society and disruption to every-day life;
- Medium (M): Threat realisation would cause moderate damage to the society;
- Low (L): Risk occurrence has little effect on society;

Likelihood of the threat to be realised:

- High (H): likely to occur; high probability that the threat would be realised
- Medium (M);
- Low (L): not likely to occur.

Impact on society
The main purpose of this criterion is the evaluation of the impact of new threats in the CC/CT field. The assessment of impact on different society areas is based on the Political, Economic, Social, Technological, Legal, Environment (PESTLE) analysis and covers a number of sub-criteria that define the threat impact for:

- Political and legal system;
- Economy;
- Social system;
- Technology;
- Environment.

Maturity
The fourth criterion estimates the time when the technology and other circumstances are sufficiently matured for the threat to be realised:

- Short term (2017);
- Medium term (2020);
- Long term (2025).

Legal and Ethical Recommendations for Research

Introduction and Approach

In order to fully appreciate the challenges and demands faced by society in respect of CC and CT it is important to analyse and understand the legal and ethical implications for conducting research and developing solutions in the area. In this section we focus on five key areas in this regard, consisting of **General Issues** (social cohesion and discrimination against gender, religion and minorities), **Victim's Rights** (fundamental rights and freedoms of victims and suspects), **Data Protection** (privacy of individuals affected by research), **Illegal Content** (legality of research) and **National Security** (confidential intelligence and information). These recommendations were developed through a four step process, with each step building on and supplementing those that preceded.

1. Research was carried out to create and present a comprehensive inventory of relevant publications. This led to a thorough overview of already existing scientific explorations and examinations of legal and ethical implications
2. Drawing from the inventory established in step 1, the general aspects were presented which are specifically relevant for each of the five key issues detailed in the following section. This included necessary and valuable definitions as well as meticulous observations and useful evaluations.
3. Recommendations for research into CC/CT were derived from the general aspects elaborated and presented in step 2 and presented in deliverable "**D2.4 Legal, Ethical and Societal Recommendations**".
4. The general aspects presented in step 2 were verified in brief studies concerning particular national jurisdictions. In so far as these selected national jurisdictions partly overlap, providing a slightly more holistic perspective on these jurisdictions in its final deliverable.

Results and Recommendations

General Issues of Social Inclusion

The general issues of gender, religion, or ethnic minority do not raise any legal issues specific to CC/CT research. However, sensitive legal issues are connected to ethical aspects of conducting sound and fair, i.e., unbiased, research and of presenting research results in a way that avoids stigmatisation of groups that are distinguished as being of particular relevance in the research.

Research project developers and managers and individual researchers are advised to:

- take particular care in the presentation and interpretation of research results to avoid stigmatisation;
- avoid biases in research design or analysis in terms of what is considered 'normal' behaviour, based on an implicit standard of white heterosexual Christian males as a reference point;
- foster inclusive formations of research groups, with an appropriate gender balance and where possible including researchers from different religious or ethnic groups, which can minimise the risk of biased research assumptions;
- ensure that individual researchers and project teams are independent and can function free from pressure from financing organisations, governments, or social pressure groups.

Victim's Rights

On balance, matters pertaining to victims' rights generate only a number of limited problems regarding future research activity on CC/CT. These legal aspects are directly linked to the correct way in which a research project is carried out and subsequently presented. Avoiding harm to the interests of those who have been affected by CC/CT, research project developers and executives and researchers are recommended to:

- pay particular attention in the presentation and interpretation of research results in order to avoid encroaching on the victim's privacy and harming their reputation or "right to be forgotten";
- Remove the possibility of identifying victim's personal data (as far as possible);
- reduce to a minimum or to the extent that it is strictly indispensable for research purposes, the use of material and information which could potentially harm victims' rights (cases of child pornography or other sexually related crimes);
- guarantee impartiality as well as extraneity on the part of researchers and to avoid any implicit or explicit personal observation on matters forming the subject matter of the research project.

Data Protection

The exemptions for research on data protection requirements are mostly specified in national secondary laws. Harmonisation at the EU level was completed in the legislative trilogue for a General Data Protection Regulation on 15 December 2015 (Draft GDPR[Trilogue]). The European Parliament has adopted the GDPR[Trilogue] as final so that the future GDPR will most likely come into force in June 2016 and become applicable tin two years time. Any international harmonisation concentrates legal barriers for research into CC/CT particularly because such research is almost inherently cross-border research. Compliance with any additional and supranational data protection regimes is essential for any research project in the area of CC/CT. Towards such data protection compliance, the following measures are highly recommended:

Anonymisation

It is recommended that data is anonymised at the earliest stage possible. Anonymisation preferably occurs prior to disclosing or using data for research purposes.

Notification

For each jurisdiction affected by a research project it has to be verified whether the data subjects have to be notified of their data being processed or whether this duty may not apply because such notification is impossible due to the nature of the research or the necessity of a disproportionate effort from the researchers.

Consent

For each jurisdiction affected by a research project it has to be verified whether consent has to be obtained from all affected data subjects or not because this would be impossible due to the nature of the research or the necessity of a disproportionate effort from the researchers.

Legitimacy of Data Processing

Each research project has to determine what type of data is used and for which purposes, which is related to the necessity of the data processing and purpose binding principles. The participants involved have to be indicated, which refers to the data subjects, but also to the data controller and possible data processors. In line with the purpose of the processing, it has to be decided for how long the data will be used, how long they will be stored, and when the data are to be deleted. Stricter rules will apply to a research project processing sensitive data (e.g. medical records or educational records).

Data Security

Researchers have to make sure that the personal data is only processed for these scientific or statistical purposes and cannot be used for other purposes. Moreover, when results from the research are published, these have to be anonymous.

Illegal Content

The legality of any research project in the area of CC/CT presupposes a clear understanding of which researched content is qualified as illegal. For research projects in the area of CC/CT the following recommendations apply:

Appropriate Risk Assessment

Researchers have to undertake an appropriate risk assessments concerning the planned research and prepare clear safety plans and processes to ensure the maximum physical, psychological and emotional safety of all those involved.

Awareness and Sensitivity to Cultural Differences

Researchers should have an awareness of and sensitivity to, cultural differences both within and between Member States; what is acceptable in one country or culture may be entirely unacceptable in another. Whether victims will talk about their experiences to a researcher, for example would depend on the stigma attached to being a victim of a certain crime, or fear of being identified by a perpetrator.

Anonymity/ Pseudonymity

Researchers should develop methods of research which are sensitive to the needs of those involved; for example one which allows for the use of anonymity and/or pseudonymity to provide reassurance and encourage participation. Also methods which transfer traditional approaches into the cyber environment which is more appropriate to the work required.

Guidelines for Each Research Project

To establish a clear set of guidelines as to what is understood to be 'illegal content'.

Towards European Research Guidance

The more research projects establish their clear guidelines the closer we get to establish a 'European legal and ethical guidance for researchers' covering all aspects of potential work. Such guidance would include issues like legal duties and ethical dilemmas, handling of data and protection of all those involved.

National Security

With regard to the absence of a European harmonisation of the understanding of national security and differences in the legal frameworks among EU member states, it is essential that research projects and researchers carefully examine any of their content whether it could potentially interfere with issues of national security prior to the start of the research project. For a research project in the area of CC/CT it is advised to apply the following recommendations:

Awareness of National Security Principles

Research in CC/CT has to be mindful about the possible interference of research as well as the publication of research results with principles of national security.

Caution with Differences in National Legal Standards

Research in CC/CT has to be also aware that legal standards related to the protection of national security differ significantly already within the EU and even more so at global level. The standards that apply in the country where research results are hosted are not necessary the same as in other countries that are involved in the research project.

Prior Analysis of Implications on National Security

Prior to any research assessment as well as the publication of any research results, a review analysing all possible implications with regard to national security has to take place.

References

Aaltonen, M., & Barth, T. (2005). How do we make Sense of the Future. Journal of Futures Studies 9.4 (2005): 45-60.

Amanatidou, E., Butter, M., Carabias, V., Konnola, T., Leis, M., Saritas, Schaper-Rinkel, P. & Van Rij, V. (2012). On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues, in Science and Public Policy 39 (2012), pp. 208–221.

Cuhls, K., van der Giessen, A.. Toivanen, H., Erdmann, L., Warnke, P., Toivanen, M., & Seiffert, L. (2015). Models of Horizon Scanning. How to integrate Horizon Scanning into European Research and Innovation Policies.

EFFLA (2013). Policy Brief N° 13, Strategic Intelligence Methodology.

Hauptman, A. & Sharan, Y. (2013). Foresight of evolving security threat posed by emerging technologies. Foresight, VOL. 15 NO. 5 2013, pp. 375-391.

OECD (2016). Futures Thinking: Overview of technologies. Available at: http://www.oecd.org/site/schoolingfortomorrowknowledgebase/futuresthinking/overviewofmethodologies.htm

Van Rij, V. et al, (2010). Joint horizon scanning: identifying common strategic choices and questions for knowledge, Science and Public Policy, 37: pp 7–18.

The COURAGE Consortium