Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions

Borka Jerman-Blažič and Tomaž Klobučar(✉)

Jožef Stefan Institute, Ljubljana, Slovenia
{borka,tomaz}@e5.ijs.si

Abstract. Cybercrime and cyberterrorism research faces a number of challenges, such as the rate of change in technology, field complexity and interdisciplinarity. This chapter aims at identifying the major technical challenges that require solutions to be developed for the successful prevention and fight against such contemporary problems. The following solutions have been elicited as a leading contribution towards the design of a cybersecurity research agenda. The identified and selected solutions include technologies and techniques for computer fraud prevention, investigation and detection methods and tools, and crime prevention methods that address human elements.

Keywords: Cybercrime · Cyberterrorism · Research agenda · Technical challenges · Fraud prevention · Data sharing · Big data · Human elements

1 Introduction

Cybercrime (CC) is one of the fastest growing forms of crime, with more than one million people worldwide becoming its victims each day. Cybercriminals and CC network attacks are increasingly present in the everyday life of civilians, organizations, enterprises and government institutions. The longer we live in a digital world, the more opportunities will be present for cyber criminals or terrorists to exploit the vulnerability of networks, organizations and human lives. In discussing CC, the appearance and the relation to cyberterrorism (CT) should be mentioned here, as the dividing line and differentiation in the research approach are not very clear and sharp. Some authors have suggested that the key feature that makes the difference between CC and CT is the motivation of the actors, as crime is considered to be driven more by "personal gain or revenge" while terrorism is driven by dominance of "political" reasons to cause damage to an organization or a political system. Addressing a particular problem and developing prevention methods and technologies for specific CC/CT attacks is usually considered an unsustainable, non-scalable and inadequate approach, as this approach does not provide protection for all facets of cyberspace. In addition, the fight against CC/CT by the relevant authorities, e.g. law enforcement

B. Akhgar and B. Brewster (eds.), *Combatting Cybercrime and Cyberterrorism*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-38930-1_9

agencies, cannot assure the envisaged security and safety without cooperation with the private as well as the public sector. These large parts of the society acting in the digital world need to adopt a different approach for the security architecture (e.g. trusted computing, ubiquitously embedded security automation technologies, information sharing). Building security as a robust and solid foundation for citizens and economic entities to conduct transactions in the digital world is a must. This finding reflects this chapter of the book intended to identify the major technical challenges that require solutions to be developed for a successful prevention and fight against CC and CT. The selection of missing solutions includes technologies and techniques for computer fraud prevention, investigation and detection methods and tools, and, crime prevention methods addressing human elements.

2 Understanding Cybercrime and Cyberterrorism

2.1 Rate of Change in Technology

Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. Today almost everyone in the world is connected either to the Internet or to some other phone network [1]. The estimated number of Internet users is close to five billion [2] and the expectations are that this will increase steadily over time. No society, no country, no individual will be unaffected in the close future [3]. The second contributor to the extreme speed of change in technology is the explosion of data. The amount of data being produced is rapidly growing and will grow ten times over the next six years, reaching 44 trillion gigabytes of data by 2020 [4] that can be stored and analysed to give unprecedented insights at macro and micro scales, allowing to understand and predict the global trends, the growing of data markets and individual behaviors. According to many sources, electronics will be embedded in everything and will enable the monitoring and control of every aspect of the current world, blending both the physical, e.g. Internet of Things, and digital worlds in an unimaginable way [5]. The pervasiveness of information and communication technology and ubiquity of digital infrastructures means that the digital civilization is now a fact of life. Some examples illustrate this: digital media, digital social relations, critical infrastructures, services, surveillance, industrial control, government, intelligent transport systems, and smart cities, amongst others. The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of information society. This development brings great opportunities and improvement to the daily life. However, this is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICT [2]. Cars, traffic control, elevators, air conditioning or telephones also depend on the smooth

functioning of ICT. Attacks against information infrastructure and Internet services now have the potential to harm society in new critical ways. On-line fraud and hacking attacks are just examples of computer-related crimes that are committed on a large scale every day [1]. The financial damage caused by CC is reported to be enormous and the damage per enterprise caused in USA only exceeds USD 15 million [6]. By some estimates, revenues from CC were outstripping the illegal trade in drugs for the first time in 2007 [2]. These estimates clearly demonstrate the importance of understanding CC and of developing effective prevention and protection methods and tools. As the major difference between CC and CT is in its dominating motivation [7], CC is generally committed for individual, personal reasons such as personal gain or personal revenge. CT attacks may have the same results and use the same methods, but the motivations are usually different. Such motivations may be aimed to destabilise an institution or country, or to intimidate a population into changing its government's behavior [8]. In that context, analysts and legislators are facing the problem of understanding the motivations of persons who carry out a cyberattack when trying to classify it and determine how the perpetrators should be prosecuted. These distinctions have a clear significance for justice and law enforcement, despite the use of similar techniques, methods and approaches for committing attacks. The techniques and some of the results are usually identical to certain instances of CC, as fundamentally any attack consists of individuals or groups seeking either to disrupt or take over communications and information systems or to extract information by tapping a wire. A key concept in this context is the "advanced persistent threat", frequently employed in espionage and cyberwarfare to continuously monitor and extract data from specific targets, using a set of stealthy and continuous hacking processes. Such long-lasting attacks require the capability, resources and intent and are thus commonly seen as requiring the resources and motivations of governmental agencies.

In the last decade many definitions appeared for CC, for example Hartel [9] defines CC as a behaviour in which computers or networks are a tool, a target, or a place of criminal activity [10]. This includes as a subject the information security, namely techniques to prevent or detect attacks on information assets, but the issue is much broader because it also includes such topics as the use of computers to commit "traditional" crime. For these reason the Global Cybersecurity Agenda [1] has seven main strategic goals, built on five work areas: (1) Legal measures; (2) Technical and procedural measures; (3) Organizational structures; (4) Capacity building; and (5) International cooperation.

It is possible that CC will become nothing special in the future. Something similar has happened before, with the introduction of new technology: The industrial revolution urbanised crime, which the law enforcement of the day was unable to cope with [11]. This eventually led to the introduction of the modern police force. We may expect also that the information revolution, especially if the speed of change is considered, will have a significant effect on law enforcement too in fighting against CC. However, before CC is subsumed by the definition of crime, there are some significant challenges to be met. For example, the Lockard's exchange principle [12] which is the foundation of forensics, does not seem to

apply to CC scene investigations. In addition, the existing technical infrastructure of the Internet has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Solutions, technical and strategic measures need to be developed to prevent attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as an adequate and sufficient legislation allowing law enforcement to prevent and fight CC effectively [13].

2.2 Complexity and Interdisciplinarity

The complexity in the prevention of CC and the fight against cybercriminals is based on several dimensions originating from the characteristics of the current digital world. CC knows no borders. The crime site where the attack happens is independent of the presence and location of the attackers. There is no need for the criminals to be present at the same location as the target. As the location of the criminal is usually different from the crime site, many cyber-offences are transnational by nature. International CC offences affect more than one country, and the protocols used for data transfer on the Internet are based on optimal routing if direct links are temporarily blocked. Even when the domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to its final destination. On the other hand, because no general control instruments exist, users are able to use filter circumvention technologies to send encrypted anonymous communication out of the country. As the number of people connected to Internet is growing, there is also a simultaneous increase of the number of offenders. As a consequence, any estimation of the number of offenders or people who use the Internet for illegal activities [2] is rather difficult. The increasing number of offenders causes difficulties for law enforcement agencies, as currently there is no possibility to automate the CC investigation process. Another problem is the short life of the data vital for tracing offences, especially in cases when cloud infrastructure is involved. The data are deleted after a short time. The short time available for investigation is problematic as the traditional mutual legal assistance regime often takes time to organise. Offenders may also include third countries in their attacks to make the investigation more difficult. Due to the complexity of the field, CC is by definition a multidisciplinary field as, among others, it makes use of mathematics, engineering, economics, medical science (psychology), sociology, criminology, law and public management [9].

3 Challenges and Threats

3.1 On-Line Anonymity and Data Protection

One of the major challenges of the fight against CC is the on-line anonymity as many Internet services are designed in such manner to make the identification of offenders difficult. The possibility of anonymous communication is either a by-product of a service, or is offered with the intention to avoid disadvantages for

the user. Some examples are public access terminals, public wireless networks, prepaid mobile phone services that do not require registration, storage capacities for homepages, anonymous communication servers and remailers. Offenders can use several tools to hide their identities, such as fake mail addresses, or use free mail servers. In order to protect user privacy, several countries support the principle of anonymity, as is the case with the EU. The data protection applied to protect information from access by unauthorized people uses encryption technologies as a key technical solution. However, the same technology is used by offenders, making it difficult for law enforcement agencies to break the encryption and access the data. The recent case with encrypted data in an Apple iPhone and the US Agency's request to the manufacturer to reveal the encryption key which was refused is a good example. The availability of encryption technologies and their use by criminals are challenges for forensic investigators and law enforcement agencies [14].

3.2 Challenges and Technical Aspects of Data Sharing

Cyber-attacks happen in all types of organizations and individuals. They can start in many different places, including any device connected to the Internet. This is highly problematic in the modern digital society where devices such as copy machines are hooked up to the Internet in order to update themselves, report usage, install software, etc. Having all these devices connected to the Internet increases the exposure and vulnerability to CC [14]. In addition, it makes information sharing between the victims and the law enforcement bodies more difficult. Due to so many targets on the Internet sharing information, among the investigation instructions and law enforcement agencies the request by stakeholders for an effective sharing of information for fighting CC is obvious. There is an urgent need to create an orderly way of looking for threats and reporting the facts found in case of committed crime in a standard and understandable way for all involved. The implementation of countermeasures, for example the intrusion detection systems (IDS), which are part of the network hardware and software, requires maintenance and updating with recent developments [15]. Information about this should be shared as well. The systems used for monitoring and tracing should be adaptive and will need to have some level of self-awareness, self-learning and self-explanation to be able to address a moving target, such as CC criminals. Some predictability will be needed based on the shared data collected from different sources that will essentially allow the understanding of crime scenarios and learning from past wrong decisions. Information sharing should be implemented also by building new awareness and methods that enable the crime trends to be recognized in their early sprouts.

3.3 Illegal Content and Underground Market

The Internet is becoming the main instrument for the trade and exchange of material containing child pornography. The major reasons for this development are the speed and efficiency of the Internet for file transfers, its low production

and distribution costs, and its perceived anonymity. Pictures placed on a webpage can be accessed and downloaded by millions of users worldwide. One of the most important reasons for the "success" of web pages offering pornography or even child pornography is the fact that Internet users are feeling less observed while sitting in their home and downloading material from the Internet. The same applies to hate speech and racism and xenophobia-motivated propaganda on the Web. The problem in that context is that not all countries criminalise hate speech [2]. An additional problem is the appearance of the Dark Web, i.e. overlay networks which use the public Internet but require specific software, configurations or authorization to access. The dark web includes marketplaces trading in mainly illicit products and services, such as drugs, software exploits (e.g. Trojan horses, botnets), network attacks offered as a service, and weapons. In addition to services such as fraud, this illegal marketplaces offer illegal and ethically disputed pornography, phishing and scam services and tumblers for Bitcoin services [16]. One of the major features of the dark web is the obscuring of the originating Internet Protocol (IP) address of its users via Tor protocol applications. The nature of activity of the Dark Web explains why little research exists related to this challenge.

3.4 Big Data, Abundance of Information and Analysis

Data sets on the Internet are growing rapidly, partly because they are increasingly gathered by cheap and numerous information-sensing mobile devices, aerial (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers and wireless sensor networks. The world's technological per-capita capacity to store information has roughly doubled every 40 months since the 1980s [17]; as of 2012, every day 2.5 Exabyte (2.5×10^{18}) of data is created [18]. The abundance of data and information within the ICT systems raises several issues related to cybercrime. This includes the protection of Internet privacy, international government cooperation, passenger name record transfers, anti-terrorism developments, freedom of information, Internet censorship, e-Identity systems, corporate governance, the appointment of privacy regulators, cross-border data flows, data retention, judicial process, government consultation procedures, information security, national security and aspects of roughly a hundred technologies and technology applications ranging from video surveillance to DNA profiling. However, sophisticated solutions for their analysis and the successful removal of the potential appearance of false answers may contribute to the development of effective cyber intelligence features, by exploiting the huge potential of currently available as well as emerging information management technologies. Emerging technologies and new analytic techniques on big data are crucial for a better understanding of the criminal strategies and the anticipating trends and they will become crucial for the prevention and fight of CC.

3.5 Human Elements

In many instances the weakest point in the ICT system's defences is the human element. CC attacks are made possible by the fact that the current security technology was developed only with an aim to protect the ICT systems, and the consideration of how real users react when exposed to malicious attacks to their assets or privacy was neglected. Developing effective protection and system defences requires an understanding about how users behave and what traits of their behaviour make them and the systems vulnerable. Understanding the aspects of human psychology exploited by criminals will enable the building of robust systems able to resist most of the known CC attacks [19]. Research into victims' issues, their rights and policy recommendations will enable the voice of victims to be transferred to government and criminal justice agencies and will contribute to the changes of the legislation and policies affecting victims and witnesses.

3.6 Challenges in Anticipating a New Generation of Cybercrime

One of the appearances of crime without borders is its spreading through the Internet, causing CC cases in all manners of appearance. This is seen as an emerging spreading phenomenon that appears and will appear in the future in different shapes and scenarios. Cybercrime is a high-profit and low-risk endeavour. A successful fight against it requires a compendium of methods for preventing and combating this type of crime [20]. The expected occurrence of new CC will be caused by not yet forecasted, not yet foreseen crime related to the auxiliary structure of the free Europe, enabling the free transport of people, goods and capital. This addresses a cross cutting new challenge where several EU and member state bodies could become partners to be aligned but also confronted with the impact of travelling criminals causing high impact or high volume crime, or will be confronted with new ways of fraud and threats without any physical travelling. Crime fighting and prevention are usually implemented in traditional ways. The low flexibility of these methods is a risk that needs to be addressed. The adaptability for new solutions is low due to the hierarchical structure and fixed and insufficient budgets. The fight against crime and crime prevention will require flexible and fast measures and resources and justly discussions on competence and ethical rules. Solutions need to be developed for "real case scenarios", recognisable for policy makers, but above all for the leaders of law enforcement agencies. In that context the following is needed:

- Forecast and understanding of fast-appearing or potential new crimes,
- Technologies that can sufficiently anticipate new trends, upcoming crimes and potential threats. The challenge and objective of using new technologies for discovering what are the rapidly evolving trends, enabling the development of new mobile and flexible methods for identifying group structures and alliances, multi-crime and different crime activities. Their use should allow the understanding and detecting of the dynamics of potential threats and crimes in a sufficiently anticipatory manner in order to be able to act in time and appropriately.

4 Missing Elements and Solutions

This section presents the missing elements and solutions required to be developed to cope with the challenges of CC and CT described above. The elements and solutions have been identified on the basis of past and on-going research activities in the field and by applying the COURAGE gap analysis methodology. The sources of information included EU projects with topics addressing CC and CT and their repositories, the IEEE Explorer, SCOPUS, Google Scholar and ProQuest databases, and organizations, such as Europol, ENISA, UNICRI, OECD, and ITU. The outputs of this analysis are later combined with the results of Chap. 3 in defining the elements of the Research Roadmap presented in Chap. 16.

4.1 Fraud Prevention Techniques

Fraud is defined as an act of deceit to gain an unfair advantage. For an act to be legally considered fraud, the attacker needs to knowingly communicate false information to the victim, and the act must affect the victim in a negative way. Computer fraud refers to "*acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data*" [3]. It thus uses electronic resources to present fraudulent or misrepresented information as a means of deception [21].

Methods to counter computer fraud can be divided into methods to detect computer fraud, and methods to prevent it. The former concentrate on analysing the system and user behaviour and detect fraud by searching for anomalies or certain deceitful characteristics. While these methods are already heavily used in some business areas, they are still an intensive research topic. Prevention of computer fraud concentrates on a fast response when detecting fraudulent actions to avoid (further) losses, as well as on policies, education and awareness, and technologies that prevent fraud related threats to be realized.

Many fraud scandals in recent years and statistics [22] show that the means to counter computer fraud are still lacking effectiveness, and that fraud detection and prevention methods are still an open field for research. In this subsection several challenges of the techniques that are used for fraud prevention are described together with missing related technical solutions, in particular the required solutions for effective and efficient protection against malware, data protection, authentication, and fraud prevention of digital currency.

Efficient and Effective Protection Against Malware
An important step in preventing computer related fraud is to protect against malicious software or malware, which is the top cyber threat [23]. Malware is becoming increasingly sophisticated, intelligent, versatile, available, and is affecting a broader range of targets and devices [22]. The increasing use of smart devices, e.g. smart phones, constitutes an opportunity for malware to steal information such as online banking login credentials and account information as well

as other data stored on mobile devices [24]. Infected mobile devices are also targets for ransomware (e.g. Locky, TeslaCrypt, Simplocker) and have the potential to act as an infection vector for other platforms and devices [22].

Malware detection mechanisms are either signature-based, detecting patterns of known malicious behaviour, or anomaly-based, detecting anomalous activities within a system. Both mechanisms have certain issues. Signature-based mechanisms cannot detect previously unknown threats, while the anomaly-based ones often have a high degree of false positives. The efficiency and effectiveness of the mechanisms is also challenged by sophisticated evasion techniques that make malware detection and analysis harder [25]. Evasion techniques can be VM-aware, sandbox-aware or debugger-aware [26], and can complicate the detection and analysis of malware in virtual security environments (virtual machines) or prevent it from deploying or running in a sandbox environment [27]. Malware, such as the UpClicker Trojan, is able to detect the context and act accordingly, for example to remain silent in case of absent activities [28]. Advanced techniques for information hiding, e.g. malware traffic, by means of steganography or through hidden channels are also expected in the near future [29] and require proper discovery technologies.

More effective and efficient protection technologies for resource-constrained devices such as mobile phones and tablets are required [30], as well as the improved detection by correlating and analysing a broader set of features from the system and network. The solutions should also be able to perform malware analysis on-line and in a non-intrusive fashion [31].

Data Protection

Cryptographic algorithms are the basic security mechanisms for protection against illegal data modification, forgery, and disclosure. A number of symmetric and asymmetric algorithms exist [32] that provide different degrees of protection against specific types of attackers, such as individuals, organizations and intelligence agencies. The security level provided depends on the selected algorithm, key sizes, parameters, usage mode, as well as implementation details [32].

While the properly implemented and used standard cryptographic algorithms can ensure an adequate security level for most of the legacy and future systems, several issues still exist. Those issues are mostly a result of the deployment of protection measures in emerging constrained environments (e.g. Internet of Things) and the new computing possibilities in the future, especially the ones expected from quantum computing.

The NIS WG3 report [33] identifies the following three main research challenges regarding cryptographic algorithms, which are also relevant for the area of computer fraud prevention:

- ultra-light algorithms for systems and devices with constraints in, for example, computational power, memory, and energy, such as sensors, moving objects and other lower-resource devices,
- ultra-high-speed algorithms,

– public key algorithms that ensure long-term security, in particular the algorithms that cannot be broken when quantum computing reaches the level of practical usability.

Several recent and past security incidents, e.g. the Heartbleed bug in the OpenSSL library, the POODLE flaw in the TLS protocol, or the FREAK weakness in some implementations of SSL/TLS, have shown the importance of an adequate design and implementation of network security protocols. Cyber criminals can exploit any flaws of the protocols to obtain illegal access to computer systems and confidential data, such as private keys, login credentials and other private data, which can be then used to impersonate a legitimate user and commit fraud.

Existing network security protocols also face different issues in constrained environments, such as the Internet of Things, low-power wireless sensor networks or ad-hoc wireless networks of moving objects with low resource capabilities. Lightweight security protocols need to be developed for those environments at network and transport layers. Security mechanisms are also required to protect end-to-end communications, and to address cross-layer security aspects [34].

From the aspect of law enforcement, data protection mechanisms and secure protocols can be seen as a technical barrier obstructing the efficient and effective fight against computer fraud. While end users use encryption algorithms to protect their data and prevent fraud, cyber criminals can exploit these to cover the traces of criminal activities [22]. An example of the use of secure network protocols for illegal activities is the use of Tor and I2P (Invisible Internet Project) networks to provide anonymity in drug marketplaces, such as the Silk Road. New peer-to-peer networks that host the command and control infrastructure are more resilient and create additional difficulties for the disruption or taking down of botnets [22]. Law enforcement is seeking new solutions to be able to gather, access and decrypt digital evidence of CC and CT activities more easily, as well as to identify offenders using anonymization technologies.

Authentication Techniques

Strong authentication methods facilitate computer fraud prevention. Despite the research on alternative authentication mechanisms in the past years, there has been little change for users in practice [35]. People still use passwords that create too much of a burden and are plagued with security and usability problems. Users choose weak passwords that can be easily broken, even if stored in a protected form. This becomes a problem especially in the cases when attackers steal millions of them from large service providers' databases [36]. Advanced and more secure authentication mechanisms need to be used by default to prevent cyberattacks or minimize their effect, and the mechanisms should be combined (multifactor authentication) in a way that is acceptable to the end users and provides a higher level of security. Also, the number of explicit authentication events for the user has to be reduced in authentication mechanisms, and advanced technologies for implicit authentication of users developed [35].

Additional research is also required for stronger authentication mechanisms for mobile systems, constrained environments and clouds. Examples of such

mechanisms are the graphical authentication for touchscreen devices, biometric authentication for mobile phones, for example the Android face unlock and iPhone fingerprint unlock [37].

Fraud Prevention and Digital Currency
Digital currency, being a sequence of bits, may be copied much easier than paper-based currency. Developing mechanisms to protect from such copies and/or fraud in general are still required for the digital currency to succeed and for confidence in digital financial systems to be developed. Methods and tools that will provide the user with strong security including some level of control over their data usage (assuring transparency on who is using what and for what purpose), while providing protection of their privacy, are needed. These tools should be able to verify who has access to the user data, and revoke this access if desired (assuming that this does not conflict with any local law) [38].

Both types of digital currency (the centralized Web and Perfect money, and the decentralized Bitcoin and Darkcoin) continue to evolve and with them the entire criminal economy [22]. The current processing power is still not sufficient for an easy decryption of the used cryptographic mechanism for digital currency creation. The development of quantum computers can contribute so this will become hypothetical. Novel cryptographic models thus need to be developed, as well as more efficient traceability tools and forensic tools for the file formats of digital currency wallets and accounts.

4.2 Operational Standards for Data Sharing

Collaboration between stakeholders such as law enforcement, public institutions and industry has been recognized as an important step in the fight against CC. However, collaborative actions in the field of CC data sharing are not trivial and easy to achieve. The heterogeneity in goals, strategies, and approaches on how stakeholders manage security issues, as well as how different sectors, for example critical infrastructure, energy, finance and banking, or public administration, manage data sharing and information exchange, must be taken into account. Companies often do not share incident related data because they are afraid their reputation would be damaged or they would lose their competitive advantage against other companies. Given the transnational nature of CC activities, different legislative frameworks in different countries make the issue even more challenging.

Several intra-sector and cross-sector initiatives have already been established to improve the sharing of cybersecurity incidents on the level of the EU and globally [39]. However, despite those initiatives, the approach for efficient knowledge sharing that would allow for a secure interoperability and collaboration between national and international bodies operating in the prevention of CC and CT is still missing. The lack of incentives from the private sector, primarily to share information on network information security issues, has been identified as an issue. As such, the scope for improving the incentivisation of cooperation and also practical mechanisms for increasing the level of information sharing between

the public and private sectors remains a key area for research. Efforts are needed for the standardization of formal representations of threats, attacks and CC incidents. Some of the problems were elaborated in several initiatives (e.g. Mitre's STIX specifications [40] and approached in the ACDC project Centralized Data Clearing House data schemata [41]. Standard protocols for threat/incidents data exchange have also been proposed, e.g. Mitre's TAXII specifications [42]. However, more work is required for an efficient provision of shared knowledge between law enforcement agencies and other stakeholders. Solutions are also missing in the following areas:

- Global standard of CC information representation/exchange formats;
- Standardization of APIs for information sharing among the shareholders;
- Models for CC and CT attacks/incidents behaviour patterns.

Finally, dynamic and semantically annotated databases/repositories of known vulnerabilities for an automatic detection of vulnerabilities in source code would be helpful. Current repositories of known vulnerabilities are kept up-to-date, but in practice when reviewing the code the checking must be done manually. There are no automated methods for matching/finding patterns in the code that are already present in the repositories of vulnerabilities [43]. Also, the information in the repositories could be used for predicting, at design time, the likelihood of including a vulnerability or security flaw in the implementation code.

4.3 Solutions for Dealing with Illegal Content, Dark Web and Virtual Cybercrime

In CC, computers and computer networks can be a tool, a target or a place of criminal activities. Places vary from mobile devices, personal computers, web servers, clouds and companies' private networks to virtual worlds, social networks and parts of Internet known as Darknet or Dark Web, accessible only by the previously mentioned anonymous communication protocols such as Tor.

The biggest portion of the Darknet seems to be devoted to illegal activities, such as stolen goods, drugs, weapons and information selling, exchange of illegal content, for example content related to child pornography, child-sexual abuse, and illegal financial transactions [16]. The technologies needed to fight those activities include technologies for exploring the Darknet, detecting and monitoring criminal activities and identifying criminals in the dedicated servers of the Darknet, and seizing illegal content. The missing solutions should provide (1) monitoring of social sites to detect message exchanges containing new Darknet domains, (2) marketplace profiling for collecting information about sellers, users and the kinds of goods exchanged, (3) locating and mapping hidden services directories by deploying nodes in the distributed hash tables, and (4) monitoring hidden services of newly added sites. New investigation approaches are also needed for decentralized marketplaces such as the OpenBazaar, a BitTorrent-style peer-to-peer network [29].

The usefulness of virtual worlds and mixed reality environments in many different fields was proven by several R&D projects and other research (e.g. GALA Network of Excellence in Serious Games). Use of well-designed mixed reality makes the actors feel that they are immersed in cyberspace. Unfortunately, virtual environments are not immune to CC activities, as shown by the increase of such activities in the past years [44]. It is estimated that millions of dollars in virtual goods are stolen in virtual worlds. Virtual worlds face also other types of criminal activities and offences, such as money laundering, extortion, stalking, or hate speech. Normative frameworks to deal with virtual crime need to be developed, including (reputation-related) offences against avatars.

4.4 Information Management of Big Data

Big data is data characterized by high volume, high variety, high velocity, low veracity and high value. Here, variety refers to different formats of structured and unstructured data, velocity to the speed of data change, and veracity to the data quality. In the cybercrime domain, big data is used both by law enforcement and criminals. On one side, emerging technologies and new analytic techniques on big data are crucial for a better understanding of criminal strategies, anticipating trends and preventing and fighting cybercrime. On the other side, criminals use big data analytics to increase the value of stolen data [22].

Big Data Collection, Processing and Use for the Detection and Prevention of Cybercrime and Cyberterrorism

Big data mining and analysis represent important techniques for the identification of potential CC threats and trends, criminal and terrorist group structures and different crime activities. The technique should enable understanding and detecting the dynamics of the threats and activities in a sufficiently anticipatory manner in order to be able to act in time and appropriately. Big data analysis should thus add predictive and proactive capabilities to the fight against CC.

Solutions are also required that can quickly provide sense based on big data to an investigator and do not leave room for misinterpretation of the analysis results. Misunderstandings can be caused by an improper use of big data for predictive analytics, especially by equalling correlation with causality. Standardised procedure and best practices are therefore needed by law enforcement for properly conducting Big Data-related investigations and interpreting results [22]. A better understanding can also be facilitated by adequate visualization techniques that are scalable in visually representing massive amounts of data from heterogeneous and distributed data sources, and capable of rendering these in real time.

Privacy Protection Issues in Big Data Management

Big data can include vast amounts of personal data collected through various sensing devices to gain insights about individuals and their environment. Personal information or personal data that need to be protected are any information relating to an individual who can be identified, directly or indirectly. An important requirement of big data management is thus the protection of personal

data, and finding a balance between the protection of privacy and the use of advanced data correlation and intelligence capabilities for cybercrime prevention, for example when conducting automatic mass video analysis. New solutions are also needed for a safe anonymization, aggregation, and deletion of stored data in a way that prevents de-anonymization and de-aggregation. The solutions should be sensitive to the contexts in which the data is considered private. They (in particular the ones that have some proactive properties) should be capable during their use to be aware of privacy issues and must be capable to control the information found or discovered in order the disclosure of private information to be minimal [38].

4.5 Human-Centred Solutions

Past experience has shown that technical solutions for prevention of and protection against CC are often too complex to use for non-experts, not convenient or not applicable for certain groups of users, and potentially privacy-intrusive. It is therefore of big importance that technical solutions in this field are human-centred, usable and able to protect user privacy.

Usability Issues
The literature review shows that additional study is needed to provide security and privacy services and mechanisms that are user friendly, without discarding the consideration of the security capabilities and performance of the service or the mechanism. The research gap needs to be tackled both from the technological and psychological points of view. Law enforcement officers need more usable and simpler tools for their daily work and investigations. Hibshi et al. highlight a number of usability issues that need to be taken into consideration when designing and implementing, for example, digital forensics tools [45]. The issues include the consistency, information overload and non-intuitive interfaces. Usability is especially critical here because misunderstanding that leads to false interpretations may impact real-life forensic cases [45].

Privacy Issues
Despite existing privacy protection services and privacy principles that should be followed when designing and developing services and systems that process personal data, e.g. privacy by design, different research issues still exist. Bettini and Riboni identified various technical, legal, user experience, and economical challenges related to privacy protection in pervasive systems [46]. From the technical point of view, they for example miss tools able to integrate and present the information about an individual held by adversaries, as well as more accurate models of adversary knowledge about a user. The proposed research directions for mobile participatory sensing include impact assessment of sensor reading combination and correlation on the user's privacy, as well as the provision of composable privacy solutions [47].

Privacy-friendly authentication and authorization mechanisms are also missing in wide deployment. STORK 2.0 has built an infrastructure for the use of strong authentication by means of national eID credentials in the EU for secure

cross-border services, such as e-banking, e-health, e-education, and e-commerce [48]. The authentication mechanism is extended with the privacy-friendly use of business attributes for authorization purposes. Privacy protection is added to the authentication and authorization procedures by anonymous credentials and some other authentication mechanisms, such as privacy-preserving attribute-based credentials [49].

4.6 Harmonization of Terms in Cybercrime and Cyberterrorism

The current terminology used among law enforcement and other stakeholders was found to be ambiguous [7]. The definitions and the topics are overlapping. Despite the high perceived levels of awareness around the general concept of terrorism, there is little consensus towards an internationally agreed definition of CT [50]. Despite numerous attempts towards establishing a common definition for CT, none have resulted in a common, agreed international consensus on the issue [51].

The absence of an equal representation of subject areas, the definition of terms and the different taxonomy proposed in the field are identified as a problem by academia, law enforcement agencies, and by entities representing legal and ethical organizations and critical infrastructures [10]. Such an absence of harmonization can cause problems at all levels, from first response and research, right through to policy formulation and the development of legislative frameworks. Clear and logical definitions in the area of CC and CT are necessary to understand, measure, and fight CC and CT. It is necessary to have a robust framework in which different aspects of CC/CT can be classified, categorized and explained within the context and the meaning. Finally, a clear definition and an exhaustive taxonomy that may lead to metadata specification are necessary.

5 Conclusion

Identifying challenges and missing solutions is an essential step in the design of a comprehensive research agenda in any domain. This chapter focused on the field of CC and CT and the contemporary challenges and solutions, due to the very nature of CC and CT the primary focus of the chapter was on technical features. The presented results facilitate a better understanding of the challenges one faces in the prevention of and the fight against CC and CT, as well as the technical elements and solutions that one still requires to be able to cope with those challenges.

Acknowledgement. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7-SEC-2013) as the COURAGE project under grant agreement no 607949.

References

1. International Telecommunication Union (ITU): Understanding Cybercrime: Phenomena, Challenges and Legal Response (2012). http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime20legislation20EV6.pdf
2. International Telecommunication Union (ITU): Understanding Cybercrime: Guide for developing countries (2011). http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
3. United Nations Office on Drugs and Crime (UNODC): Comprehensive Study on Cybercrime (2013). http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
4. Bisson, P., Martinelli, F., Granadino, R.R. (eds.): Cybersecurity Strategic Research Agenda (2015). https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/
5. Hui, S., Jiafu, W., Caifeng, Z., Jianqi, L.: Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering, Proceedings, pp. 648–651 (2012)
6. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T., Savage, S.: Measuring the cost of cybercrime. In: Böhme, R. (ed.) The Economics of Information Security and Privacy, Chap. 12, pp. 265–675. Springer, Heidelberg (2013)
7. Sims, D., Ghernaouti, S.: A report on taxonomy and evaluation of existing inventories. D2.1, E-CRIME deliverable (2014). http://ecrime-project.eu/
8. Koops, B.J.: The internet and its opportunities for cybercrime. In: Manual, T.C., Herzog-Evans, M. (eds.) vol. 1, pp. 735–754. WLP, Nijmegen (2010)
9. Hartel, P., Junger, M., Wieringa, R.: Cyber-crime Science = Crime Science + Information Security, University of Twente, Version 0.15 (2010)
10. Newman, G.R.: Cybercrime. In: Krohn, M.D., Lizotte, A.J., Penly Hall, G. (eds.) Handbook on Crime and Deviance, pp. 551–584. Springer, New York (2009)
11. Newman, G.R., Clarke, R.V.: Superhighway Robbery: Preventing E-Commerce Crime, pp. 8–9. Willan Publishing, Uffculme (2003)
12. Brenner, S.W., Clarke, L.L.: Distributed security: preventing cybercrime. John Marshall J. Comput. Inf. Law **XXIII**(4), 659–667 (2005)
13. Helfgott, J.B.: Criminal Behaviour Theories, Typologies and Criminal Justice, pp. 4–18. SAGE Publications, Thousand Oaks (2008)
14. Lipson, H.P.: Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Requirements for Next-Generation Internet (2002). http://www.sei.cmu.edu/reports/02sr009.pdf
15. Oehemen, C., Peterson, E., Dowson, S.: An organic model for detecting cyber-events. In: CSIIRW 2010 Proceedings of the Sixth Annual Workshop on Cybersecurity and Information Intelligence Research, Article No. 66. ACM, New York (2010)
16. Moore, D., Rid, T.: Cryptopolitik and the Darknet. Survival **58**(1), 7–38 (2016). doi:10.1080/00396338.2016
17. Hilbert, M., López, P.: The world's technological capacity to store, communicate, and compute information. Science **332**(6025), 60–65 (2011). doi:10.1126/science.1200970
18. Boyd., D., Crawford, K.: Six Provocations for Big Data, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society (2011). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431

19. Victim support. https://www.victimsupport.org.uk/more-us/policy-and-research/
20. Horizon 2020, Secure Societies Advisory Group, Strategic Input for 2016-2017 Workprogram, April 2015, Private communication (2015)
21. Kunz, M., Wilson, P.: Computer Crime and Computer Fraud. University of Maryland, College Park (2004)
22. European Cybercrime Centre (EC3), Europol - The Internet Organised Crime Threat Assessment 2014 (iOCTA) (2014)
23. Marinos, L.: ENISA Threat Landscape 2014: overview of current and emerging cyber-threats. ENISA (2014)
24. Choo, K.-K.R.: The cyber threat landscape: challenges and future research directions. Comput. Secur. **30**, 719–731 (2011)
25. Marpaung, J.A.P., Sain, M., Lee, H.-J.: Survey on malware evasion techniques: state of the art and challenges. In: 14th International Conference on Advanced Communication Technology (ICACT) (2012)
26. Ortega, A.: Your malware shall not fool us with those anti analysis tricks. AlienVault Labs (2012)
27. Arntz, P.: Sandbox sensitivity. Malwarebytes unpacked (2013). https://blog.malwarebytes.org/intelligence/2013/02/sandbox-sensitivity/
28. Singh, A.: Don't Click the Left Mouse Button: Introducing Trojan UpClicker. FireEye Blog (2012)
29. European Cybercrime Centre (EC3), Europol - The Internet Organised Crime Threat Assessment 2015 (iOCTA) (2015)
30. Suarez-Tangil, G., Tapiador, E.J., Peris-Lopez, P., Ribagorda, A.: Evolution, detection and analysis of malware for smart devices. IEEE Commun. Surv. Tutorials **16**(2), 961–987 (2014)
31. Chen, P., Desmet, L., Huygens, C.: A study on advanced persistent threats. In: De Decker, B., Zúquete, A. (eds.) CMS 2014. LNCS, vol. 8735, pp. 63–72. Springer, Heidelberg (2014)
32. Agency, E.U., for Network, Information Security (ENISA): Algorithms, key size and parameters report - 2014 (2014)
33. Kert, M., Lopez, J., Markatos, E., Preneel, P.: State-of-the-art of Secure ICT Landscape (Final, Version 1), NIS Platform, Working group 3 (WG3) (2014)
34. Granjal, J., Monteiro, E., Sá Silva, J.: Security in the integration of low-power wireless sensor networks with the internet: a survey. Ad Hoc Netw. **24**, 264–287 (2015)
35. Sasse, M.A.: "Technology should be smarter than this!": A vision for overcoming the great authentication Fatigue. In: Jonker, W., Petković, M. (eds.) SDM 2013. LNCS, vol. 8425, pp. 33–36. Springer, Heidelberg (2014)
36. Mirante, D., Cappos, J.: Understanding password database compromises. Polytechnic Institute of NYU, Technical report TR-CSE-2013-02 (2013)
37. Bhagavatula, C., Ur, B., Iacovino, K., Kywey, S.M., Cranor, L.F., Savvides, M.: Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. USEC 2015 (2015)
38. European Union Agency for Network, Information Security (ENISA): ENISA Report on Strategic Research Agenda, draft v02.63 (2014). https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents

39. European Union Agency for Network and Information Security (ENISA): ENISA cybersecurity Information Sharing: An Overview of Regulatory and Non-regulatory Approaches (2015). https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing/at_download/fullReport
40. MITRE: Structured Threat Information eXpression (STIX) specification (2014). http://stix.mitre.org
41. Advanced Cyber Defence centre (ACDC) (2016). https://www.acdc-project.eu/
42. MITRE: Trusted Automated eXchange of Indicator Information (TAXII) specifications (2014). https://taxiiproject.github.io/
43. Torres, R., Gallego-Nicasio, B., Zanetti, R.: Initial set of research activities listed to meet gaps. CAPITAL (cybersecurity research agenda for privacy and technology challenges) D3.1 deliverable (2014)
44. Adrian, A.: Beyond griefing: virtual crime. Comput. Law Secur. Rev. **26**(6), 640–648 (2010)
45. Hibshi, H., Vidas, T., Cranor, L. Usability of forensics tools: a user study. In: Sixth International Conference on IT Security Incident Management and IT Forensics, pp. 81–91. IEEE (2011)
46. Bettini, C., Riboni, D.: Privacy protection in pervasive systems: state of the art and technical challenges. Pervasive Mob. Comput. **17**, 159–174 (2015)
47. Christin, D.: Privacy in mobile participatory sensing: current trends and future challenges. J. Syst. Softw. (2015). doi:10.1016/j.jss.2015.03.067
48. Klobučar, T., Gabrijelčič, D., Pagon, V.: Cross-border e-learning and academic services based on eIDs: case of Slovenia. In: eChallenges 2014: 29–30 October, 2014 Belfast, Ireland. Dublin: IIMC: = International Information Management Corporation, 9pp (2014)
49. Camenisch, J., Dubovitskaya, M., Enderlein, R.R., Lehmann, A., Neven, G., Paquin, C., Preiss, F.-S.: Concepts and languages for privacy-preserving attribute-based authentication. J. Inf. Sec. Appl. **19**(1), 25–44 (2014)
50. Record, J.: Bounding the Global War on Terrorism. Strategic Studies Institute (2003). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA419754
51. Jarvis, L., Nouri, L., Whiting, A.: Understanding, locating and constructing cyberterrorism. In: Chen, T.N., Jarvis, L., Macdonald, S. (eds.) Cyberterrorism: Understanding, Assessment and Purpose, pp. 25–41 (2014) doi:10.1007/978-1-4939-0962-9