A systematic approach toward description and classification of cybercrime incidents

George Tsakalidis and Kostas Vergidis
Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece

Abstract

The advancements in computer systems and networks have created a new environment for criminal acts, widely known as cybercrime. Cybercrime incidents are occurrences of particular criminal offences that pose a serious threat to the global economy, safety and well-being of society. This paper offers a comprehensive understanding of cybercrime incidents and their corresponding offences combining a series of approaches reported in relevant literature. Initially, the paper reviews and identifies the features of cybercrime incidents, their respective elements and proposes a combinatorial incident description schema. The schema provides the opportunity to systematically combine various elements – or cybercrime characteristics. Additionally, a comprehensive list of cybercrime-related offences is put forward. The offences are ordered in a two-level classification system based on specific criteria to assist in better classification and correlation of their respective incidents. This enables a thorough understanding of the repeating and underlying criminal activities. The proposed system can serve as a common reference overtaking obstacles deriving from misconceptions for cybercrimes with cross-border activities. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that match with the offence type and subsequently with a particular incident. This matching will enable better monitoring, handling and moderate cybercrime incident occurrences. The ultimate objective is to incorporate the schema-based description of cybercrime elements to a complete incident management system with standard operating procedures and protocols.

1.Introduction

Cybercrime involves a mixture of diverse typical crimes with new illegal acts. Individual cybercrime incidents are occurrences of particular criminal offences and, as multiple national crime statistics and surveys demonstrate, are steadily

increasing [1]. According to the Federal Bureau of Investigation [2], the Internet Complaint Center received 269,422 complaints of Internet crime in 2014, which indicates a rise of 1600% in comparison to the 16,838 complains included in the initial report [3]. In a worldwide study released by PricewaterhouseCoopers [4], the number of reported information security incidents around the world rose 48% in 2014, the equivalent of 117,339 attacks per day. Similarly, the German Crime Statistics indicated a 23,6% increase in the number of cybercrime incident from 2007 to 2008 [5].

The various offences of cybercrime pose a serious threat to the global economy, safety and well-being of the society. In a PricewaterhouseCoopers [6] report it is highlighted that cybersecurity incidents are not only increasing in number but they are also becoming progressively destructive and target a broadening array of information and attack vectors. This advancement poses a serious threat to the operations of businesses, organizations and national economies as the global financial damage is estimated around $225 billion [7]. Moreover, the impact of cybercrime offences to individuals is also immense; from identity theft to sexual exploitation of children and cyber-harassment, the various cybercrime offences provoke from a slight discomfort to severe mental harm, public fear and financial loss [8].

Due to its complex nature, a series of definitions of cybercrime exist in literature and in different agencies responsible to tackle it. The U.S. government does not have an official definition of cybercrime that distinguishes it from common criminal offences. Similarly, there is not a definition of cybercrime that differentiates it from other forms of cyber threats, and the term is often used interchangeably with other Internet- or technology-linked malicious acts such as cyberwarfare, and cyberterrorism [9].

A more coordinated attempt aiming to the perception of a widely accepted definition was proposed in the Convention on Cybercrime [10] . In the summary of the Treaty [11], cybercrimes are defined as 'crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security'. In the accompanying explanatory report [12], cybercrimes are also referred to as 'cyber-space offences' that are 'either committed against the integrity, availability, and confidentiality of computer systems and telecommunication

networks, or they consist of the use of such networks of their services to commit traditional offences.' Nevertheless, even though this implementation is relatively thorough, there are considerable gaps regarding the specification of each feature of the above definition.

Another issue in relation to understanding cybercrime is the lack of a concise classification and monitoring of the particular offences it entails. The term 'cybercrime' encompasses a broad range of criminal activities that are complex in nature, constantly evolving and utilizing new means of invasion. As a result, a classification system to categorize and match the various cybercrime incidents to corresponding offences and thus take the necessary actions and apply appropriate policies, is considered essential for effective incident management.

Gordon and Ford [13] proposed a typology consisted of two categories: Type I offences characterize singular or discrete events facilitated by the introduction of malware programs such as keystroke loggers, viruses and rootkits. Type II offences are facilitated by programs that are not classified as crimeware and there are generally repeated contacts or events from the perspective of the user. A much broader classification, was recommended by Wall [14] proposing three distinct categories. The first is *Computer Integrity Crimes* including the illegal activities of cracking, hacking and denial of service. In the second category of *Computer-Assisted Crimes* the offences of virtual robberies, scams and thefts are included. The third category is *Computer Content Crimes* including pornography, violence and offensive communications.

In regards to monitoring of computer-related offences, organizations and agencies such as EUROPOL, FBI and ENISA compose annual reports for cybercrime and cyber threats, bringing about threat trends on a yearly basis. However, it is arduous undertaking to quantify the impact of computer-related offences on societies, on the basis of the number of offences carried out in a given time-frame [15]. Another important fact about these statistics is that they deal with cybercrimes that are detected and reported [16], which can lead to the assumption that the actual number of cybercrimes is significantly larger. Also, many of these reports do not provide a direct matching of particular offences with concrete actions, counter-measures and policies that are appropriate and essential for the elimination of particular cybercrime incidents.

The multiple interpretations of what cybercrime entails along with non-systematic classification of the corresponding offences and lack of recommended actions are not contributing towards managing and orchestrating effective directives, policies and legislative initiatives at local, national or international level and result in ineffective handling of cybercrime incidents. This paper aims to contribute towards better understanding cybercrime by proposing a schema-based cybercrime incident description that: (a) identifies the features of a cybercrime incident and their potential elements, and (b) provides a two-level offence classification system based on specific criteria. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that counteract the offence type and subsequently the particular incident. This matching will enable better monitoring, handling and moderating the various cybercrime offences and their incarnation in the form of specific incidents.

2. Feature identification of cybercrime incidents

The issues with providing a comprehensive description about cybercrime incidents are two: (a) there is already an adversity in existing cybercrime definitions that focus on different aspects, and (b) the incidents that can be classified as cybercrime demonstrate a significant variety in their features and characteristics (e.g. offender, target, means of attack). To tackle the issues above, the authors propose a hybrid schema-based incident description that adapts accordingly to encompass and describe accurately the various cybercrime incidents. Having such a mechanism enables: (a) a better understanding of a specific incident, (b) accurate classification and monitoring of the corresponding criminal offence and (c) effective action in terms of counter-measures and policy generation.

The first step towards the schema is to determine the basic *features* of a cybercrime incident. Table 1 presents eight identified features that describe an incident in a comprehensive way. Each of the identified features answers a basic question about an aspect of the incident (e.g. what happened?) and it is provided along with a brief description and the feature name. The first feature ('*incident*') is the initial description of the incident itself (e.g. illegal downloading of movie files). The second feature ('*identified offence*') answers to the question on whether this particular incident is considered criminal activity and under which criminal offence it can be classified. The third feature ('*offender*') specifies the individual or entity responsible for the offence that took place, whereas the fourth feature ('*access*

violation') is unique to cybercrime offences as it highlights the way that a computer or a network was misused and violated for the cybercrime incident to be carried out. The next three features ('*target'*, *victim'*, *'harm'*) describe the aim of the cybercrime incident along with those that suffered and the consequences (individual, systemic and inchoate harm) sustained.

no.	***incident feature***	***feature description***	***answers the question***
1	INCIDENT	description of the incident	*what happened?*
2	IDENTIFIED OFFENCE	criminal offence that occurred	*is it considered criminal activity? which one?*
3	OFFENDER	individual or entity that is responsible for the incident	*who is responsible?*
4	ACCESS VIOLATION	computer/network violation approach	*how it occurred?*
5	TARGET	values that are the desired target	*what was targeted?*
6	VICTIM	individual or entity that has suffered	*who has suffered?*
7	HARM	the caused harm	*what was the harm induced?*
8	ACTIONS, MEASURES & POLICIES	recommendations for the particular incident	*what can be done to tackle and prevent it?*

Table 1. Identified features of cybercrime incidents

The final feature that the authors suggest is not directly linked with the description of the incident itself but ties it to: (a) immediate actions to handle it, (b) specific measures to prevent similar offences and (c) elaborate policies that suggest formal action towards a specific category of cybercrime. The authors believe that it is important to properly assign cybercrime incidents to criminal offences utilizing a systematic approach and also allocate specific actions, measures and policies so that an incident is properly addressed in all levels –from immediate actions to national policies. Especially for cybercrime offences with high frequency of occurrences this can prove quite helpful as a guide. However, this last feature requires further investigation and it is not analyzed further in this paper.

Having recorded the various features that accurately describe a cybercrime incident the next step is to identify the various elements of each of the features to accurately describe a cybercrime-related incident. By identifying the elements of each feature we can then further examine any interrelations between specific elements that would highlight specific aspects of cybercrime offences.

Incident

The first feature is a brief generic description of a particular incident that has occurred. Assigning it specific elements –from a set of already occurring incidents- would limit our capacity to describe new, future or more sophisticated incidents. Therefore, this feature will remain generic and it will be further specified and clarified by the remaining of the proposed features.

Identified offence

For an incident to be considered illegal, it has to be classified under an existing criminal offence. By grouping the various cybercrime incidents to corresponding offences the authorities can devise systematic and effective ways of tackling cybercrime in a timely manner. The challenge with cybercrime incidents is that they might include aspects of various known offences, they are complex in nature and they are still evolving in novel unprecedented occurrences. Table 2 presents an indicative list of cybercrime offences that an incident can belong to. It is evident however that the list is neither conclusive nor comprehensive. The challenge with offences is two-fold: (a) a thorough classification system of cybercrime-related offences and (b) a set of specific criteria for assigning a specific criminal incident under one or more particular offences. The next section of this paper presents the authors' proposal based on the above-mentioned challenge.

IDENTIFIED OFFENCES	
Child Pornography	Illegal Interception
Computer-related forgery	Misuse of devices
Computer-related fraud	Phishing
Copyright-related offences	Pornographic Material
Cyber laundering	Racism and hate speech on the Internet
Cyberwarfare	Religious Offences
Data Interference	Spam and related threats
Identity theft	System Interference
Illegal Access (hacking, cracking)	Terrorist use of the Internet
Illegal data acquisition (data espionage)	Trademark-related offences
Illegal gambling and online games	

Table 2. Indicative list of cybercrime-related offences

Offender

The offender is the individual or entity that is responsible for carrying out or participating in a criminal incident. The offender can either be an individual, a group of individuals or an entity as table 3 shows. This approach derives from the

separation of the actual attacker and the one being the instigator of the attack. This means that in an information war between two countries, despite the fact that a group of trained individuals carries out the attack, the actual offender is the country instigating this act. Table 3 presents the elements of the feature 'offender' that are briefly discussed below. The authors ascribed the title of offender to the specific categories of individuals and entities, following ENISA's 2015 Threat Landscape [17]. These threat agent types are the top initiators of cyber-incidents. For incidents that do not derive from threats to cyber-security, i.e. content-related offences, the authors have introduced additional types of offenders.

Abusive user: This category of offenders includes racists, anti-Semites, homophobics, xenophobics, religious offenders and any other internet users with the intention to insult the values and provoke others beyond the legal boundaries. These users propagate hate speech on the Internet and glorification of violence, with the false alibi of the right to freedom of expression. Unfortunately, one of the negative sides of the Internet is that it composes a global forum for the advocates of intolerance and inequality [18].

Individual	Entity
Abusive user Cyber-bully Cyber-criminal Cyber-fighter Cyber-terrorist Hacktivist Insider (employee) Online social hacker Script kiddie Sexually deviant user	Company / Organization Country / State

Table 3. Types of offenders in a cybercrime incident

Cyber-bully: A lot of media attention is focusing on cyberbullying incidents due to the serious consequences that can lead to the victim committing suicide. Cyber-bullies intend to insult, hurt or embarrass other individuals through sending or posting text or images through the Internet, cell phones or other devices [19]. Their practices differ as they may be limited to posting rumors or gossips on the Internet. The cyber-bully may reach the extent of publishing sensitive material causing severe defamation and humiliation.

Cyber-criminal: Cyber-criminals are responsible for most of the incidents as their main purpose is to obtain intelligence and profit from illegal and criminal activity in the world wide web. They are typically involved in fraud regarding every possible cyber activity such as: e-commerce, scareware, ransomware, development of malicious code and tools, e-finance, cybercrime-as-a-service [20]. In order to achieve their goals, cyber-criminals are highly skilled, well equipped and usually form organized groups when the target is highly profitable [21].

Cyber-fighter: Cyber-fighters are politically motivated groups of citizens, similar to hacktivists, acting on behalf of their governments and therefore contributing to the cyber activity of their country [22]. They possess remarkable striking power due to national funding and launch their attacks whenever their national, moral or religious values are offended by other groups.

Cyber-terrorist: Cyber-terrorists are a constantly rising threat agent with multiple areas of activity [23]. The Internet provides the opportunity to terrorists to recruit personnel, establish communication channels throughout the world, and raise money in forms of donations and account deposits [24]. Cyber-terrorists seek to launch cyber-attacks against critical infrastructure; however, such an attack has not been recorded as of yet.

Hacktivist: This is a threat agent group with great media attention due to their political motivation. Their main objective is hacking and unveiling critical information from organizations, authorities, politicians and people with power in general [25]. They set out to raise public concern by disseminating information to the media, promoting in this way the freedom of expression.

Insider (employee): Insiders are motivated by revenge, profit, extortion or sabotage and play a key role in many cyber threats, particularly those leading to data breaches [26]. Insiders may by current or former employees, current or former service providers/consultants/contractors or suppliers/partners, according to a PricewaterhouseCoopers report [27]. What is really important in order to minimize the risk of an insider threat, is the proper evaluation and distribution of access rights within a company, organization or public service.

Online Social Hacker: This threat agent group uses the skills and knowledge of its members regarding social engineering. The online social hackers have a deep understanding of social behavior and user emotional states and they are capable in

creating fake trust relationships with their victims. Although not using sophisticated software tools, the actions of these offenders may result in significant impact especially in areas of identity theft, collection of confidential personal data, user credentials and cyber bullying [28].

Script Kiddie: Due to the increased cybercrime visibility, the means for utilizing attacks are widely accessible. As a result, children and teenagers are attracted to such activity either for demonstration of skills [29], or just for enjoyment. Many cyber incidents have been ascribed to minors such as the TalkTalk data breach [30].

Sexually deviant user: This category encompasses offenders using the Internet to facilitate non-contact offences, such as downloading and distributing child pornography [31] and illegal pornographic material. These offenders use a variety of common technologies to exploit or abuse children, including social networking sites, peer-to-peer platforms, email, instant messaging, web cams, bulletin boards and mobile phones [32]. As sexually deviant users, can also be considered users accessing irregular pornographic material, such as bestiality, rape and torture.

Entities as offenders: The entities indicated as offenders, form a threat agent group with interrelated motivations and similar courses of actions, and hence will be introduced together. According to Higgins [33], cyber espionage at a national level is becoming a global trend for political, nationalistic, and competitive gain. During the last years, web-based attacks became a popular and effective measure in geopolitical conflicts and in gathering intelligence for economic competitive reasons.

Access violation

Access violation answers the question of how the incident took place. The authors' approach combines physical tampering with the logic of direct(overt)-indirect(covert) integrity threat of computer systems [34]:

Physical Tampering: This type of attack includes the deliberate physical damaging or corrupting of hardware devices with the intention of destruction or malfunction.

Local Computer Access: Through local computer access, an individual can log in a computer system, navigate through the operating system and carry out a series of possible attacks such as malware installation, information leakage, identity theft, data breaches, etc.

Remote Computer Access: Most of cybercrime incidents are committed remotely due to the perceived safety, impunity and anonymity that the world wide web provides. An individual with unlawful intentions, e.g. launching a web-based attack or accessing child pornography, usually commits the incident through a remote connection. The Internet, Telecommunication networks and the Dark Web are most frequently used, while private networks (intranets) accessible only to an organization's staff can also be exploited.

Target

A cybercrime offender targets to specific values depending on the victim, the nature of the attack and their objectives. These values are separated in two main categories, one regarding individual targets that refer to people or entities (e.g. companies and organizations), and the other one describing social targets like infra-structure and community. These categories are presented in Table 4.

INDIVIDUAL					SOCIAL	
Physical Abuse	**Emotional Abuse**	**Sexual Abuse or exploitation**	**Financial abuse or exploitation**	**ICT abuse or exploitation**	**Infra-structure ICT abuse or exploitation**	**Social abuse**
Provocation of physical assault, battery or murder	-Mental anguish -Offending of dignity, privacy, reputation, safety, sanity, serenity, trust -Coercion to impair one's freedom of religion or faith	Obscene or pornographic photographing, filming, or depiction of sexual assault, sexual battery, molestation or rape.	Unauthorized use/management of funds, assets, property, intellectual property or resources	Improper use/ management of ICT regarding availability, confidentiality, integrity or security	Cease or interruption of perpetual functionality through ICT abuse.	-Afflicting prosperity, stability and welfare -Inaccessible services to civilians

Table 4. Clustering of offender's targets

Physical abuse: In cybercrime offences, offenders threaten victims and provoke physical assaults, battery or murder through telecommunications and social media. This prerequisite is the key element that differentiates this type of abuse it from the crimes of assault, battery, and aggravated assault.

Emotional abuse: When offenders target a person's emotional state, their aim is dignity, privacy, reputation, safety, sanity, serenity and trust, while for entities the abuse is related to privacy, safety and reputation. Moreover, offenders also push victims into changing moral beliefs and religion. The most common offences motivated by emotional abuse are religious, racism and hate speech on the Internet.

Sexual abuse or exploitation: This kind of abuse is restricted to the content-related cybercrimes of pornographic material and child pornography, in which offenders conduct obscene pornographic photographing, filming, or depiction of sexual assault, sexual battery, molestation and rape [35]. The victims include both minors and adults, this illegal industry is extremely profitable and the cross-border character is more than evident.

Financial abuse or exploitation: In this subcategory, the offender's objective is the unauthorized use or management of funds, assets, property, intellectual property and resources in general. The targets are usually monetary and the victims also undergo emotional abuse as a result of the financial loss.

ICT abuse or exploitation: Offenders may conduct attacks against the availability, security, confidentiality and integrity of data, computer systems and telecommunication infrastructures.

Infrastructure ICT abuse or exploitation: This target refers to ceasing or interrupting the perpetual functionality of critical infrastructure, by abusing their ICT systems. Offenders aim to society in general by potentially hitting infrastructure of great importance.

Social abuse: Cybercrime offenders also target fundamental social principles by afflicting prosperity, stability and welfare or limiting accessibility to social services. They usually have the same aspiration with infrastructure ICT abuse and aim to large-scale consequences with international impact.

Victim

A cybercrime victim is either individual when reffering to a person, α company/organization, or a Country/State that has been hurt, damaged or suffered as a result of the offender's actions. The identified victims of computer-related offences are:

- ❒ *Individual*
- ❒ *Company / organization*
- ❒ *Country /State*

Harm

According to Brenner [36] both cyber and traditional crimes share essential commonalities and therefore crime metrics can be extrapolated to cybercrimes as they both inflict harm either individual, systemic or inchoate. The possible harm that can result from cybercrime incidents is presented in Table 5.

Individual Harm	Systemic Harm	Inchoate Harm
Emotional distress/fear Loss of life Loss of property Moral harm Physical injury Substantial damage/loss	**Aggregated Individual Harm** Accumulated loss of property, moral harm, emotional distress or fear from multiple individual victims of the same offence. **Generalized individual harm** Deterioration of life quality Civil disturbance Social disorder Moral decay Dispossession of wealth Violation of social relationships Economic depression **Direct Systemic Harm** Chaos and anarchy Erosion of essential government functions Critical infrastructure shut down Country engagement in armed conflict	Inferential inchoate harm Potential inchoate harm

Table 5. Incurred harm as a result of a cybercrime incident

Individual harm lies at the core of traditional crimes such as murder, theft, assault and can also be inferred in computer-related offences due to similarities in nature. This harm is actual and discrete and can be inflicted to either human beings or entities. The nature of individual harm varies from moral harm, emotional distress and fear, when referring to people and to substantial damage and loss of property regarding entities. Lastly when cybercrime offences provoke violence, the harm can extend to physical injuries or even loss of life.

Systemic harm affects society and infrastructure. As Brenner proposes [36], there are three types of systemic harm: (a) aggregated individual harm, (b) generalized individual harm and (c) direct systemic harm. In an example where a large scale online fraud takes place involving 2000 victims and €2.000.000 losses, both aggregated individual harm in terms of accumulated losses in property for the individuals successfully victimized, and also generalized individual harm regarding civil disturbance, and quality of life in society are caused. The generalized individual harm crucially affects the balance of society and can have many forms such as social disorder, deterioration of life quality, moral decay, economic depression and violation of social relationships. As direct systemic harm, the authors consider harm with immediate impact to society such as the one inflicted by a cyberterrorist that attacks a particular social system or infrastructure. Specifically, in this category is chaos and anarchy, erosion of essential government functions, critical infrastructure shut down and engagement of a country in armed conflict.

Inchoate harm is the harm inflicted by inchoate cybercrimes. It is obvious that there is no actual harm resulting from these crimes as they have not been completed, but they embody a potential for harm that is illegal according to criminal law. The two types of inchoate harm are, inferential and potential. When a fraudster sends out phishing e-mails, apart from individual harm to the ones successfully victimized, the offender sought to inflict, but failed to do so to those that did not respond, which is characterized as inferential inchoate harm. For example, online posting of police officers' personal information can lead to their injury [37] which appertains to the residual category of potential inchoate harm.

3. Classification system for cybercrime offences

The previous section stressed the need for a comprehensive classification of the cybercrime offences in order to understand, classify and combat particular incidents. This section introduces an offence classification system based on two levels. The first level consists of the four different types of cybercrime offences introduced in the Convention on Cybercrime [10] with the authors' addition of a new type: the combinational offences. For each level-1 offence type, there are level-2 sub-categories based on further analysis by Gercke [38]. The authors propose this two-level consolidation of cybercrime offence along with appropriate modifications and updates in order to provide a comprehensive cybercrime offence classification

system. The level-1 classification of cybercrime offences provides a set of five generic categories or types as follows:

Type A: Offences against the confidentiality, integrity and availability of computer data and systems

Type A includes the core of computer-related offences, offences against the confidentiality, integrity and availability of computer data and systems, representing the major threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed [12]. The types of crime covered are mostly unauthorized access and illicit tampering with systems, programs or data.

Type B: Computer-related offences

Type B includes cybercrime offences in which computer and telecommunication systems are used as the method to attack specific legal interests that are mostly protected already by criminal law against attacks using traditional means. Computer-related fraud and forgery have been added by following suggestions in the guidelines of the Council of Europe Recommendation No. R (89) 9 [39].

Type C: Content-related offences

This type encompasses the offences that require the use of computer systems as a medium and entail abusive content. It includes sexual exploitation of children, illegal pornography, religious offences and cyberbullying, offences with content considered abusive for most western countries.

Type D: Offences related to infringements of copyright and related rights

This type of offences was included in the Convention Treaty [10] because copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern.

Type E: Combinational Offences

Due to increasing Law Enforcement collaboration and public concern-alert, offenders improvise and progress their methods in order to maintain their effectiveness. Criminal activities such as cyber laundering, phishing and terrorist use of the Internet cover acts that combine a number of different offences in sole acts, which necessitates the introduction of this category.

level-1	level-2
Type A **Offences against the confidentiality, integrity and availability of computer data and systems**	A1. Illegal Access (hacking, cracking) A2. Illegal data acquisition (data espionage) A3. Illegal Interception A4. Data Interference A5. System Interference A6. Misuse of devices
Type B **Computer-related offences**	B1. Computer-related forgery B2. Computer-related fraud B3. Identity theft
Type C **Content-related offences**	C1. Pornographic Material C2. Child Pornography C3. Religious Offences C4. Cyberbullying C5. Illegal gambling and online games C6. Spam and related threats C7. Racism and hate speech on the Internet
Type D **Offences related to infringements of copyright and related rights**	D1. Copyright-related offences D2. Trademark-related offences
Type E **Combinational Offences**	E1. Phishing E2. Cyber laundering E3. Cyberwarfare E4. Terrorist use of the Internet

Table 6. Proposed classification of cybercrime offences

It is important to highlight that the proposed classification system is not based on a unique criterion that is used to distinguish the different types. Three types (A, C, D) focus on the object of legal protection whereas type B focuses on the method used to commit the crime. This can, in some cases, lead to overlapping between categories which is expected when taking into account the diversity of offences. However, the extent of overlapping is limited compared to other classification systems. Also, the authors updated the level-2 classification of offences in relation to Gercke's analysis, so as to incorporate their point of view, and simultaneously provide a contemporary and consistent list. Examples include the transferring of the offence 'Misuse of devices' from Type B to Type A, because it may require a computer system to occur, but the exclusive motive of the misuse is unauthorized access and illegitimate tampering.

According to Gercke [38], as content-related offences were also categorized 'Libel and false information', which the authors regard as ones of lower esteem and relatively difficult incrimination, not needing to come under a discrete sub-category. In this category however it was essential to add the offence of 'cyberbullying' because this social problem has erupted at the same time as social media showed up. Table 6 presents the two levels of proposed offence classification system. For each identified offence, the authors provide a detailed description based on literature review findings.

Type A: Offences against the confidentiality, integrity and availability of computer data and systems

The criminal offences defined under Type A, are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalize legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices [12].

A1. Illegal Access (hacking, cracking)

In accordance with the federal Computer Fraud and Abuse Act [40] hacking is the offence in which someone knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct aims for personal benefit. For instance, offences that are described as hacking, are the mass sending of 'spoofing' emails that contain malicious software such as key loggers (which recover every keystroke), port-scanners and rootkits, the setting of websites that intend to acquire users' passwords, breaking the security code, or gaining access to databases of password-protected websites. Especially, the information accessed may be manipulated or distributed, while the websites and accounts may undergo denial-of-service attacks (DoS) in order to crash. Furthermore, there has been an outburst of politically motivated attacks through distributed malware targeting either organizations [41] or individuals.

A2. Illegal data acquisition (data espionage)

The ubiquitous use of the Internet and the ability to access critical financial, political and personal this information through wired and wireless devices, has aroused the interest of offenders for data espionage. The means of illegal data acquisition are the same ones used for illegal access, plus some non-technical ones such as 'phishing' and 'man-in-the-middle attack' (MITH), which use methods of 'social engineering'. According to Hardy et al. [41], social engineering appears to be

of greater importance, for the offenders, than the technical sophistication of the malware attached. Lastly, relatively new but very effective are the Advanced Persistent Threats (APT) which refer to a combination of stealth processes, aiming to a particular entity. This attack is launched by skillful agents and its main purpose is to illegally acquire data leaving no traces behind. The adversaries' mission is well organized, following strict directives and guidance [42]. The alarming feature of APT though, is that they are used against sensitive State, military and industrial organizations, and that the exploitation and evasion techniques used, are mostly unknown (zero-day) to the security community [43].

A3. Illegal Interception

This category comprehends illegal interceptions of computer data and every type of digital communication (such as emails) between users. According to the Office of the UN High Commissioner for Human Rights (OHCHR) et al. [44], illegal interception of computer data is the offence in which the offender intercepts nonpublic transmissions of computer data to, from or within a computer system including electromagnetic emissions from a computer system carrying such computer data. This interception also has to be without right and be carried out using technical means. This offence can take place either on the physical or network layer. The offender targets any communication infrastructure such as rooting devices, fixed lines, wireless transmitters and on the network layer, services like chat, e-mail, VOIP, teleconference, SIP etc. An intelligent and rapidly expanding type of interception, involves the deceiving naming of a wireless access point by offenders, so that users connect to it, and they gain access to sensitive information. The fraudulent access point is named after nearby wireless access points that seem normal such as City WAPs, bars, restaurants, cafes, hotels etc.

A4. Data Interference

The data stored in computer systems are extremely important for individuals, companies and administrations, which leads to the conclusion that every unauthorized modification or access constraint would be crucial. Nowadays accessing data can be accomplished also remotely, through cloud-based platforms, which means that physical contact with the system is not necessary for the offender. According to the Convention on Cybercrime Summary [11] this offence involves the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right. These acts can be easily conducted through

distributed computer viruses combined with lack of suitable protection of the system targeted.

A5. System Interference

Alternatively, offenders target the computer systems and their seamless operation instead of the data stored in them, as this has the same result with the offence of data interference. System Interference can be achieved either through physical attack or remotely with the use of computer worms, denial-of service (DoS), distributed denial-of-service (DDoS), HTTP POST DoS, Application-layer floods, Slow Read attack, etc. Remote attacks can be conducted with the use of computer worms. A computer worm is a malicious software that duplicates itself, using system resources, in order to spread and overpower the computer system. Often, it uses a computer network to augment, aiming to security holes and breaches, that are flaws or susceptibilities in a system that can be exploited. Subsequently, worms hinder the smooth running of the computer system or network, depending on the 'payload' they encapsulate [45]. Other well-known forms of web-based attacks are denial-of-service (DoS) attacks. These either try to crash services or flood them, in order to prevent legitimate users from accessing them. The targeted computer system is flooded with numerous requests, resulting in system crash and hereupon unavailability of services, data stored, etc.

A6. Misuse of devices

According to the Office of the UN High Commissioner for Human Rights (OHCHR) et al. [44], a person commits the criminal offence of misuse of devices, when he or she, without right and intentionally produces or by any means makes available a device, computer, password or similar data for the purpose of committing the criminal offences mentioned above. Additionally, the same offence is carried out, when a person possesses any of the devices, passwords, access codes or similar data, with intent that it be used for the purpose of committing any of the above offences, regardless of who produced them, As accented in the details of Convention on Cybercrime Treaty [46] the possession shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession is not for the purpose of committing those offences. The proper tools used to commit misuse of devices have evolved especially, for relatively simple offences. The only tools needed are a computer system with Internet access, but when the attack is complex, sophisticated software personalized to the victim are necessary. Using

these software tools, the offenders have the opportunity to decrypt encrypted communication, inject computer viruses and hack a computer system only with the press of a button.

Type B: Computer-related offences

The offences in this category need a computer system in order to be conducted. They are distributed in three classes: computer-related forgery, computer-related fraud and identity theft.

B1. Computer-related forgery

This offence is about fraud and related activity in connection with identification documents, authentication features, and information [47]. The composing of a document that fraudulently appears to originate from a legitimate author, the modification of an image or video for defamation or as a proof in front of juries, and the alteration of a document or text in order to deceive, are examples of computer-related forgery. Forgery plays a key role in the success of other cybercrimes such as phishing, in which the victim is encouraged to disclose sensitive personal or financial information. This can be achieved by gaining the victim's trust regarding the sender's authenticity with the use of proper forgery techniques.

B2. Computer-related fraud

The types of Internet fraud that law enforcement agencies mostly observe are Internet Auction Fraud, Non-Delivery of Merchandise, Credit Card Fraud, Investment Fraud, Internet pyramid schemes and Advance Fee Schemes. The most common are Internet auction fraud and non-delivery of merchandise, due to the outbreak of e-commerce websites. Inevitably, users stumble upon unreliable websites and scam retailers when trying to obtain a product, regardless of the constant efforts done by law enforcement officials and Internet auction houses. According to Dolan [48] it has not been perceived as a serious problem for a number of reasons including the relatively small monetary losses that the victims suffer, the supposition of victims that law enforcement will not assist them, a feeling of embarrassment, and not knowing how to report this type of fraud. Another typical computer-related fraud is advanced fee scheme that occurs when the victim pays money to somebody in anticipation of receiving something of greater value, and then receives little or nothing in return. The advance fee

schemes may involve the sale of products or services, the offering of investments, lottery winnings, 'found money,' or many other 'opportunities.' The offenders will offer to find financing arrangements for their victims who pay a 'finder's fee' in advance.

B3. Identity theft

The increasing growth of the requirement of identifiability contributed towards the increase in identity theft, as some sought to use it in frauds and others considered the theft as the only way to hide their own identity [49]. Due to this outburst, the Federal Trade Commission in 2000 labeled identity theft as the fastest growing crime of our time [50]. As stated by Paget [51] identity theft is used to describe the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive. There are three separate phases in committing the offence of identity theft. Firstly, the offender illegally obtains information regarding the victim's identity with the use of either physical method such as stealing data from storage devices and mail theft, or with the use of search engines, malicious software, insider's attacks, and phishing through social engineering. At the second phase, the offender can take advantage of the identity information, by selling for example credit-card records to others. Lastly, the third phase, involves the use of the identity information which most of the times leads to new offences such as forgery, financial fraud and falsifications [52].

Type C: Content-related Offences

This category encompasses all offences considering matters of illegal content such as pornographic material distribution and access, child pornography and insults of religious symbols. At this point we have to underline the fact that in each country, judiciary and legislators have to consider the regional moral and cultural principles, during their duty. This entails that a national approach can, in fact, interfere with the legal system of another country, obfuscating the labeling of these offences and consequently the law enforcement procedure. According to article 10 of the European Convention on Human Rights [53] the freedom of expression is the right to hold opinions and receive and impact information and ideas without interference by public authority and regardless of frontiers. On the other hand, this fundamental right is subject to certain restrictions that are 'in accordance with law' and 'necessary in a democratic society', among others for the prevention of disorder or crime, and for the protection of the reputation or rights of others [54].

Towards this direction is also the approach of the Johannesburg Principles on National Security [55], in which it is stated that the right to freedom of expression 'may be subject to restrictions on specific grounds as established in International law, including for the protection of national security'. This vague state of affairs has led to numerous offences, as the preponderance of west societies believe that the freedom of expression is above restrictions.

C1. Pornographic Material

Due to Internet's nature, pornographic material can be easily distributed throughout the world with extreme advantages for retailers of pornographic material. According to Ropelato [56] the 12% of the websites on the Internet are pornographic, which is translated in 4.200.000 sites, involving live streaming, downloading, adult chat rooms, instant messaging, etc. Throughout the world, depending on the society's tolerance, framers have criminalized pornography to different extent. For example, accessing a porn website and exchanging pornographic material is legal for adults in most west countries, but the access is prohibited for minors because of the potential negative influence in the child's mentality and development. This exposure to pornography is most times unintentional, as children either stumble upon it when searching for information, or when they receive a pop-up advent while doing something else, pornographic images appear to interrupt an ordinary activity. However, 10% of Internet users between 9 and 19 have sought out pornography on the Internet on purpose [57].

C2. Child Pornography

Child pornography use is constantly attracting attention as a result of the availability and distribution of this content through the Internet. Unfortunately, the detected offenders probably represent only 'the tip of the iceberg' as most child pornography offender remain undetected [58]. Despite this, numbers of detected online sex offenders have drastically increased since the early 2000, as have the resources available for detecting these online sexual offences. Most detected online sex offenders are convicted of downloading or possessing child pornography [59]. According, however, to Seto et al. [58] a history of child pornography offences is a valid diagnostic indicator of pedophilia, which arouses a huge concern when combined with the limited detection rates. Illegal content with sexual intercourse involving children, cannot apparently be available to anyone as the retailers would easily get arrested. In order for the transaction to be carried out safely for both sides, most material is exchanged in forums requiring former registration and

sanction. As a consequence, Law Enforcement personnel seeking offences has little chances to gain access, unless it carries out undercover operations.

C3. Religious Offences

A constantly rising number of websites presents material related to religion that in some countries is considered abusive. An example of this material is a pejorative written statement for religious matters or a satirical cartoon publication of a religious symbol. The Internet provides to individuals the opportunity to express opinions without having to reveal their identity. This is, among others, due to the convenient registration to the majority of websites even using false personal information, and to anonymity in commenting. Freedom of expression though has a key role in the Internet's success, and such material is distributed daily from well-known sites, authors and bloggers. However even though a content publication is considered legitimate in one country, this material can be accessed from countries with stricter regulations, with a potential expostulation.

C4. Cyber bullying

The Internet is a useful implement for kids and teenagers regarding social interaction and collaborative learning experiences. Nevertheless, apart from excitement and adventure, it can be extremely dangerous, as users are a few keystrokes away from harming other [60]. Most researchers agree that the use of internet or telecommunication networks are compulsory in cases of cyberbullying and in contrary to common bullying. However, there are considerable difficulties in the actual conceptualization due to the fact that cyberbullying can take numerous forms and take place in every possible venue [61]. According to von Marées and Petermann [62], it is the intentional, continuous and aggressive action or behavior carried out by an individual or a group, through information or communication technologies. The most prevalent methods used by bullies are bullying through text messages, phone calls, emails, instant messaging and social media sharing. With respect to the consequences to victims, many of them develop reduced educational performance, difficulties in proper socialization and affective disorders [63], similar to the consequences of common bullying.

C5. Illegal gambling and online games

The regulation of online gambling varies between countries, providing an opportunity for illegal businesses to act. The most online casinos are hosted in countries with deficient legislation regarding online gambling, in order for them to

operate seamlessly. Law enforcement agents face great difficulties in tracking and incriminating those users, especially when they leave no trace of illegal activity, change the logging location and use false identities. In 2012, the European Commission adopted the Communication 'Towards a Comprehensive European Framework on online gambling', accompanied by a staff working paper [64]. This Communication sets out a methodology to enhance clarity on online gambling issues across the E.U for national authorities, related industries, operators and consumers [65].

C6. Spam and related threats

Spamming is the massive emission of unsolicited messages that mainly purport to advertisement, the most widely recognized form of which is email spam. According to the Messaging Anti-Abuse Working Group and others [66], from July 2009 to December 2010, abusive email ranged from about 88% to 91% in a total of 200 billion unaltered emails delivered from 500 million mailboxes. These metrics show that the majority of emails can be considered spam pointing out the severity of the problem. The offenders choose spamming to go after their objective, on the grounds that email distribution is inexpensive as the marginal cost for each electronic message is essentially zero. Moreover, the origin of spam messages is often difficult to determine, due to the use of unknown domains and the proper concealment of the message source [67]. Regarding the consequences, apart from annoying and distracting users, spam messages result in direct financial loss for companies, reduced productivity and breach of individual privacy [68].

C7. Racism and hate speech on the Internet

The Internet is breeding ground for radical groups to spread their propaganda, as it is a relatively regulation-free environment and their audience is global. Thus, numerous racism and hooligan groups, neo-Nazi and other far-right organizations coordinate their acts through Internet websites. The Simon Wiesenthal Center [69] affirmed the existence of at least 7000 such websites in 2007, and bearing in mind Internet growth of the last decade, this number is nowadays fiction. The extent to which this activity is considered illegal, differs among the countries throughout the world, depending on how freedom of speech is interpreted. Therefore, during the Convention on Cybercrime [10] an agreement could not be reached regarding a common position on the criminalization of xenophobic and racist Internet activity. Consequently, an additional protocol was developed, addressing solely racist and xenophobic propaganda and aiming also at improving

the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention Treaty in this area.

Type D: Offences related to infringements of copyright and related rights

In this category, offences regarding copyright and trademark infringements are discussed. Through Internet, individuals and companies distribute any type of files including products and media files, as part of a legitimate transaction. Unfortunately, all this intellectual property can be downloaded, copied and distributed, and therefore is subject to counterfeiting and copyright violations in general.

D1. Copyright-related offences

The introduction of digitalization in the media sector, apart from highlighting the prominent role of the companies and institutions as providers of entertainment content, has also opened the door to new copyright violations [70]. File sharing, uploading and downloading of files, music, movies and games has flourished in the last 20 years, but experience has shown that the right holders do not consent to much of this activity, as it is most of times illegal and no payment is received. The detractors of file sharing assert that it may diminish the range of culture on offer and pare the opportunities for talents, which combined with the depletion of investment resources, could make cultural production practices inadequate for society's needs for a wide variety of content [71]. File sharing relies on networks formed by computers, with the ability to transfer data. The network services are mostly peer-to-peer based and following the installation of proper software, users can share, search for and download files of any type [72]. The difficulties Law Enforcement agents confront during investigations vary and constantly evolve. One of them, is the fact that many countries have exceptions in usage that allow limited use of copyrighted material without the explicit agreement of the right holders, which exhibits the territorial efficacy of Copyright laws. Another one is the anonymous communication provided by recent versions of file-sharing systems [73], making user tracing extremely difficult, if not impossible.

D2. Trademark-related offences

The offences related to trademark rights include the use of trademarks in illegal activities, taking advantage of the good reputation a brand name or a well-known firm has. For example, during a spam, the offender can seek to deceive the victim with the use of a fraudulent trademark and consequently obtain valuable

information through phishing. Such combinational offences though, will be the subject of the next forthcoming section. Another implementation of trademark-related offences is cybersquatting, in which the offender illegally registers a domain name similar to a brand name. Consequently, the cybersquatter precludes the company or owner from using their brand name, which they likely spent a great amount of time building. The trademark owner is therefore unable to take advantage of his own brand name, which may lead to considerable profit loss [74]. Offenders seek to sell the domain to the rightful owner for a high price, or to use it by selling counterfeits to misled customers through their supposed connection to the legitimate company.

Type E: Combinational offences

The last category of cybercrimes includes combination of offences that have already been mentioned in the four previous types. Complex scams may encompass many different consequent offences, which highlights the necessity for this type of offences. The most representative and common combinational offences are phishing, cyber laundering, cyberwarfare and terrorist use of the Internet.

E1. Phishing

The offence of phishing is a form of social engineering through which the attacker obtains sensitive information by fraudulently pretending to be a trustworthy third party [75]. The attack is mainly conducted with the use of spoofed emails, or through the installation of malware on the victims' computers, however other methods may exist deriving from the attacker's imagination and technical expertise. Consequently, the victims perceive these emails as legitimate providing sensitive information such as credit card and e-banking account numbers and passwords, thus, circumventing every possible security measure. It is of no interest whether a computer system is equipped with highly sophisticated firewall, anti-virus and encryption software and authentication mechanisms, if the individual using it falls for the phish. Phishing as a digital offence may seem to be a variant of spam, and therefore categorized in the content-related offences. Nonetheless, this kind of attack leads to extensive losses regarding sensitive intellectual property, customer information by companies, identity theft, national security secrets and trademark violations, illustrating its' combinational character [76].

E2. Cyber laundering

The Internet provides multiple methods for money-laundering, due to its characteristics that attract criminals. For example, an offender can hide his identity, pretending to be someone else by means of IP spoofing, Wireless Fidelity technology, unprotected rooter connections and the use of pre-paid phones as modems. Moreover, financial transactions are depersonalized as no face-to-face contact is necessary, and funds can be rapidly transferred throughout the world with little or no expense. Another great advantage for offenders is the fact that several jurisdictions and legal systems are usually involved in the case of cyber-laundering offences, as they are often cross-border activities [77]. Because of the growing demand for micro-payments and the problematic use of credit cards, virtual currencies were developed in the last 20 years, providing the opportunity for Internet users to engage in criminal activity. One of the most widespread actualizations of cyber laundering is through virtual currencies, such as Bitcoin that uses peer-to-peer technology. The cyber launderer takes advantage of its decentralized character, as no central intermediates are used to ensure the validity of transaction [78]. Furthermore, the offenders use inaccurate information while registering to hide their true identity which restricts the ability of law enforcement to identify suspects by following money transfers, for example in cases related to child pornography [79].

E3. Cyberwarfare

Cyberwarfare also referred to as electronic warfare, cyberwar or information war, is used to describe the usage of information technologies in conducting warfare through the web, having tremendous advantages such as the ability to take down an enemy without getting involved in a fight. In addition, attacks using ICT are generally cheaper and faster than ordinary military attacks, and can even be conducted by small states [80]. In April 2007 Estonia came under cyber-attack in the wake of relocation of the 'Bronze Soldier of Tallinn', a Second World War memorial [81]. This act apart from street riots, led to coordinated computer-related attacks originating from multiple countries. Initially Russia was accused as the instigator of the attack [82], further analysis though, unveiled the participation of computers situated in 178 countries [83]. These attacks targeted mainly government and private sector official websites and online services, causing major economic instability. Nonetheless, because of the fact that neither of the attacks constituted an act of force, nor occurred within a war conflict between two countries, they cannot be safely characterized as cyber warfare.

Another important incident regarding cyber warfare, took place in July 2009 and the countries targeted were North Korea and the United States. The attack included three rounds of coordinated DDOS attacks against major government, media and financial websites [84].

E4. Terrorist use of the Internet

Computers seized in Afghanistan were proven to being used for preparation of 9/11 attacks, either for collecting intelligence on targets, or for sending encrypted messages via the web [85]. This highlights the web's vital role in the preparation of real world attacks, due to anonymity, numerous command and control mechanisms, and a relatively safe environment for terrorists to plan and coordinate attacks, along with critical information regarding potential targets. Terrorists also use the Internet to raise funds for their activities. The immediacy of Internet combined with its constant evolvement opens up a great opportunity for considerable financing through donations [86]. Terrorist organizations have resorted to methods such as fake web shops to hide their identity, and therefore avoid discovery [87]. Lastly, by hacking the computer and communication networks of critical infrastructure, terrorists can achieve their goals and induce civil disturbance, huge financial damage, and possibly chaos. A state's sustainability and stability is highly depended upon the perpetual and abiding functionality of infrastructure, such as telecommunication systems, electric plants, water supply systems, transportation and financial institutions [88].

4. Schema-based description of cybercrime incidents

Having described the proposed features and their particular elements that are required for a holistic description of a specific cybercrime incident, the authors propose a comprehensive schema-based incident description that combines the identified features. Table 7 presents the overview of the identified features, their respective elements and their classification in subsequent offences based on the classification system of the previous section.

Table 7 can assist in combining various elements and accurately describe a specific cybercrime incident by offering a series of scenarios at hand. The authors argue that this can be a significant step towards selecting appropriate actions and counter-measures to tackle an incident.

features	*elements*				
INCIDENT	*description of the incident*				
IDENTIFIED OFFENCE	*type A*	*type B*	*type C*	*type D*	*type E*
	A1. Illegal Access A2. Illegal data acquisition A3. Illegal Interception A4. Data Interference A5. System Interference A6. Misuse of devices	B1. Computer-related forgery B2. Computer-related fraud B3. Identity theft	C1. Pornographic Material C2. Child Pornography C3. Religious Offences C4. Cyberbullying C5. Illegal gambling and online games C6. Spam and related threats C7. Racism and hate speech on the Internet	D1. Copyright-related offences D2. Trademark-related offences	E1. Phishing E2. Cyber laundering E3. Cyberwarfare E4. Terrorist use of the Internet
OFFENDER	*Individual*		*Entity*		
	Abusive user Cyber-bully Cyber-criminal Cyber-fighter Cyber-terrorist	Hacktivist Insider (employee) Online social hacker Script kiddie Sexually deviant user	Company / Organization Country / State		
ACCESS VIOLATION	Physical Tampering	Local Computer Access	Remote Computer Access		
TARGET	*Individual*				*Social*
	Physical abuse	*Emotional abuse*	*Sexual abuse or exploitation*	*Financial abuse or exploitation*	*ICT abuse or exploitation*	*Infrastructure ICT abuse or exploitation*	*Social abuse*
	Provocation of physical assault, battery or murder	Mental anguish Offending of dignity, privacy, reputation, safety, sanity, serenity, trust Coercion to impair one's freedom of religion or belief	Obscene or pornographic photographing, filming, or depiction of sexual assault, sexual battery, molestation or rape.	Unauthorized use/management of funds, assets, property, Intellectual Property or resources	Improper use/ management of ICT regarding availability, confidentiality, integrity or security	Cease or interruption of perpetual functionality through ICT abuse.	Afflicting prosperity, stability and welfare Inaccessible services to civilians

VICTIM	Individual	Company/organization	Country /State
HARM	*Individual harm*	*Systemic harm*	*Inchoate harm*
	Emotional distress/fear Loss of life Loss of property Moral harm Physical injury Substantial damage/loss	Aggregated individual harm Generalized individual harm Direct systemic harm	Inferential inchoate harm Potential Inchoate harm

Table 7. Overview of the identified cybercrime incident features and elements

To more effectively combine the elements presented in table 7, the authors propose a specific ordering and combination of the incident features in the schematic description:

A cybercrime [INCIDENT] is an [IDENTIFIED OFFENCE] committed by the [OFFENDER(S)], conducted through [ACCESS VIOLATION], against the [TARGET] of [VICTIM(S)] resulting in [HARM], {and can be tackled with [ACTIONS / MEASURES / POLICIES]}.

The illegal downloading of a movie *[incident]* is a copyright-related offence *[identified offence]*, committed by a cyber-criminal *[offender]*, conducted through the Internet *[access violation]* against the intellectual property *[target]* of a company *[victim]*, resulting in loss of property and potential inchoate loss of property *[harm]*.

The hacking of a power plant's communication networks *[incident]* is terrorist use of the Internet *[identified offence]*, committed by cyber-terrorists *[offender]*, conducted through the Internet *[access violation]* against (a) the perpetual functionality and (b) welfare *[target]* of (a) critical Infrastructure and (b) a country *[victim]*, resulting in infrastructure shut down, erosion of essential government functions and State disorder *[harm]*.

Internet Drug Trafficking *[incident]* is computer-related fraud *[offence identity]*, committed by cyber-criminals *[offenders]*, conducted e.g. through the dark web *[access violation]* against the health, sanity and property *[target]* of individuals *[victim]*, resulting in loss of property, social disorder, deterioration of life quality, inferential inchoate loss of property and potential inchoate loss of life *[harm]*.

The hacking of a smartphone *[incident]* is the offence of illegal access *[identified offence]*, committed by a cyber-criminal, script kiddie or online social hacker *[offender]*, conducted through the telecommunication network or internet *[access violation]* against the property and smartphone availability, integrity and confidentiality *[target]* of an individual *[victim]*, resulting in loss of property, substantial damage and emotional distress *[harm]*.

Distributing any depiction of a child engaged in sexually explicit conduct *[incident]* is a child pornography offence *[offence identity]*, committed by a sexually deviant user *[offender]*, conducted through the internet *[layer of attack]* against the health, sanity, dignity and serenity *[target]* of an individual *[victim]*, resulting in physical injury, emotional distress, moral harm, deterioration of life quality and potential inchoate moral harm *[harm]*.

Table 8. Sample descriptions of cybercrime incidents based on the proposed schema

Table 8 demonstrates as series of five incident examples that are described based on the above description. It is evident that a specific incident and its impact are more accurately and holistically depicted when the specific elements of its features are detailed. Moreover, this approach allows the examination of possible dependencies and interrelations between the various elements. Discovering such dependencies between specific elements can provide a clearer perspective on particular cybercrime offences. The investigation on dependencies is presented below grouped based the types of offences (A, B, C, D and E) because it is more probable to discover interrelations based on similar criminal offences.

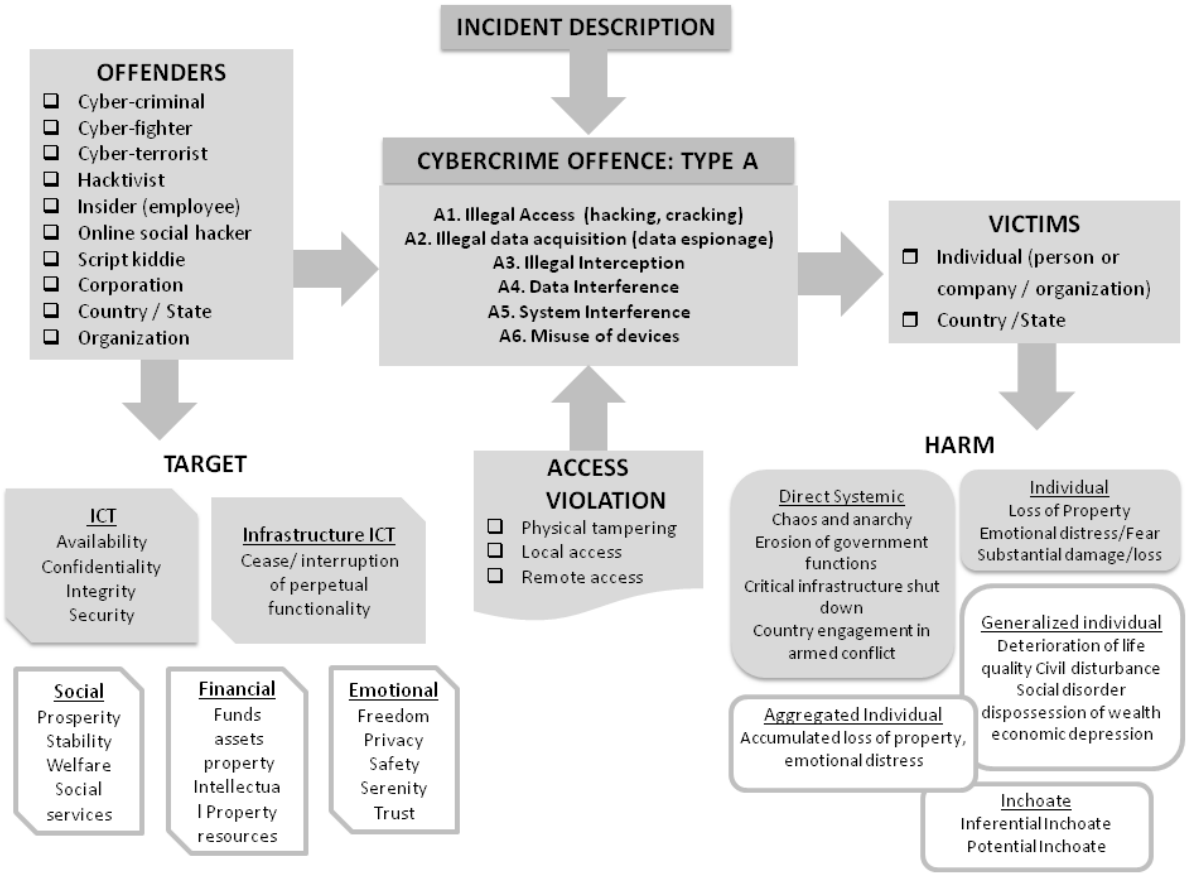

Figure 1. Incident description schema for type A offences

Type A offences pertain to criminal activity that involves the requisite targeting of information and communication technologies. What can be highlighted is that the actual target is almost always non ICT-related, as the offender's objective is to eventually gain profit, damage morality or social values. It is obligatory though that the initial target is ICT either of individuals or entities, or as part of an infrastructure network for the attack to be considered cybercrime. Moreover, as indicated in schema, the harm imposed has two levels of effect. The first immediate level is composed of individual harm, such as instant loss of property and substantial damage, and direct systemic harm which is any harm with instant large scale consequences like shutting down of critical infrastructure and failure of a government function. Subsequently, as time passes, aggregated and generalized individual harm arise e.g. in the form of civil disturbance and social disorder. It is also possible that potential inchoate harm is caused, as for example data illegally acquired can be used at a later stage, leading to individual harm.

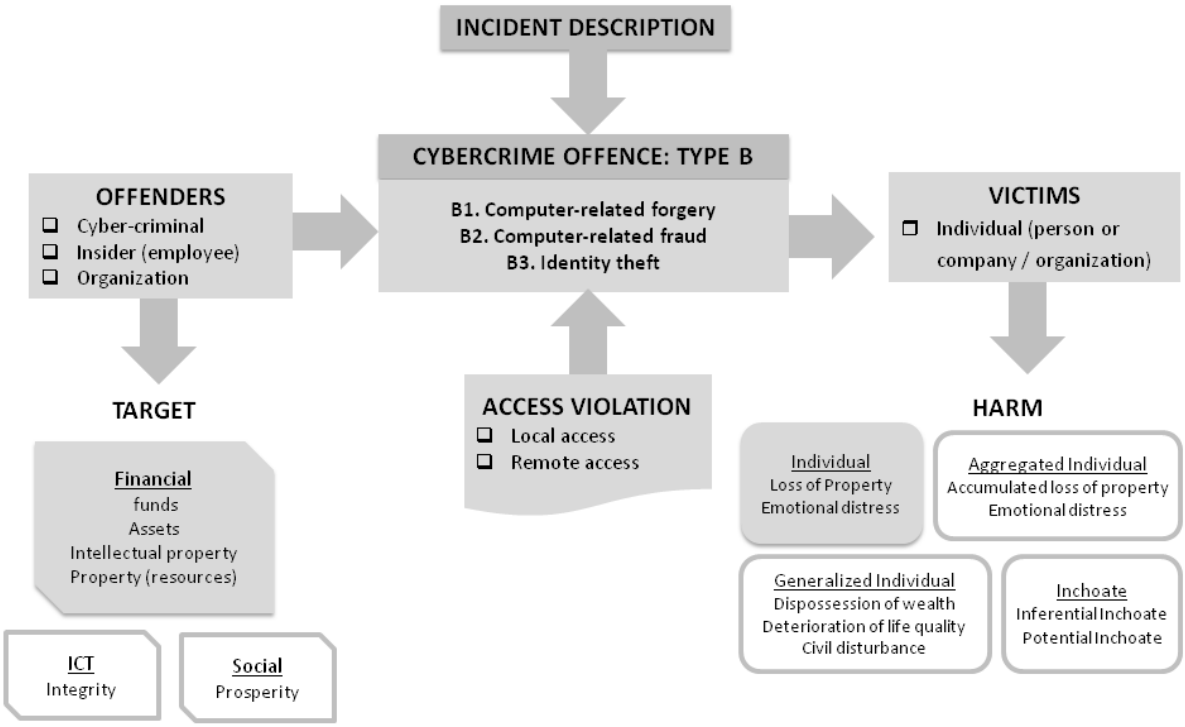

Figure 2. Incident description schema for type B offences

Cybercrimes labeled under type B are narrower regarding the type of offenders as they can only be cybercriminals, insiders (employees), companies or organizations, while victims can be individuals or companies. This is due to the financial purposes of most type B offences. As indicated in the previous section, identity theft can either aim to instant profit gain or actual identity camouflage for

activities also involving illegal profit. Regarding computer-related forgery the targeted values are amongst others monetary, through meddling with data integrity, while computer-related frauds have a clear profit perspective. The harm of type B offences is likewise restricted to loss of property and the emotional distress implied by this loss. In terms of society, there is aggregated individual harm when e.g. completed frauds have multiple victims with similar monetary losses. The generalized harm is often due to dispossession of wealth and is often in the form of deterioration of life quality. The potential inchoate harm is primarily related to identity theft offence, where the illegally acquired sensitive information can be used in the future.

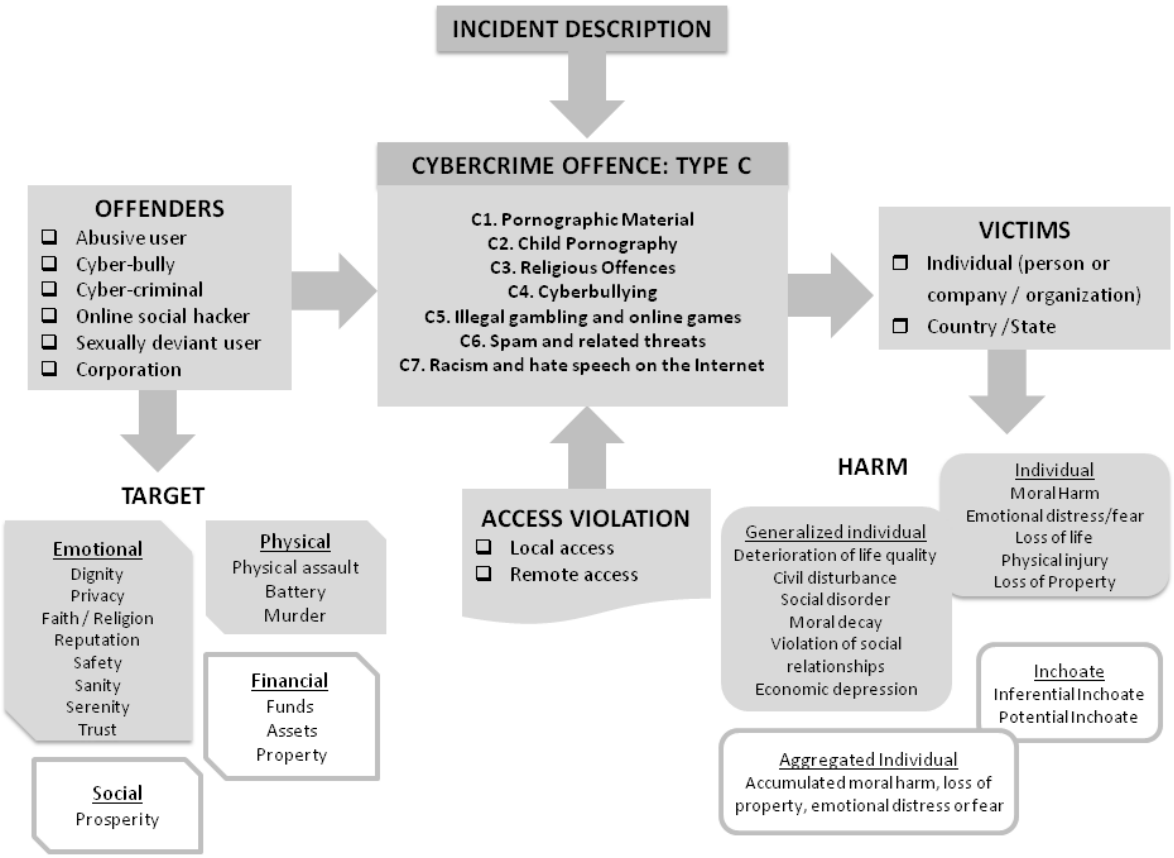

Figure 3. Incident description schema for type C offences

Type C offences are described as content-related and describe illegal incidents with emotional/psychological background. The offenders are more often cyberbullies, abusive, sexually deviant users and online social hackers while victims are mainly individuals. The cybercrimes of illegal online gambling and spam distribution are the only ones with financial objective which entails the victimization of countries, concerning national funds and assets. Emotional abuse or exploitation is the main target of this type, and involves the offending of principles like dignity, reputation,

safety and sanity while religious offences in particular, assist the impairment of freedom of religion and faith. Moreover, cyberbullying, illegal pornographic material and child pornography also comprehend physical abuse or exploitation, as offenders provoke physical assault, battery or even murder. Sexually deviant users are responsible for sexual abuse or exploitation, as they seek to view or distribute photographs, films or depictions of sexual assaults, battery, molestation or rape of both adults and minors.

This prompts criminals to commit these illegal acts and provide them as a service through online 'real time' pornography. Regarding to harm, it is mostly imposed to individual's morality with the consequences being emotional distress, fear and moral harm, while physical abuse can cause physical injury and in extreme conditions loss of life. In offence types of illegal online gambling and spam distribution, loss of property is the main harm inflicted to victims. Type C offences also lead to generalized harm such as moral decay, violation of social relationships and civil disturbance, gradually deteriorating the quality of civilian life. Lastly, systemic harm is also in form of aggregated individual harm, while the inchoate one is in this case potential harm which will be evident as time passes, e.g. in the morality of a child having undergone sexual molestation.

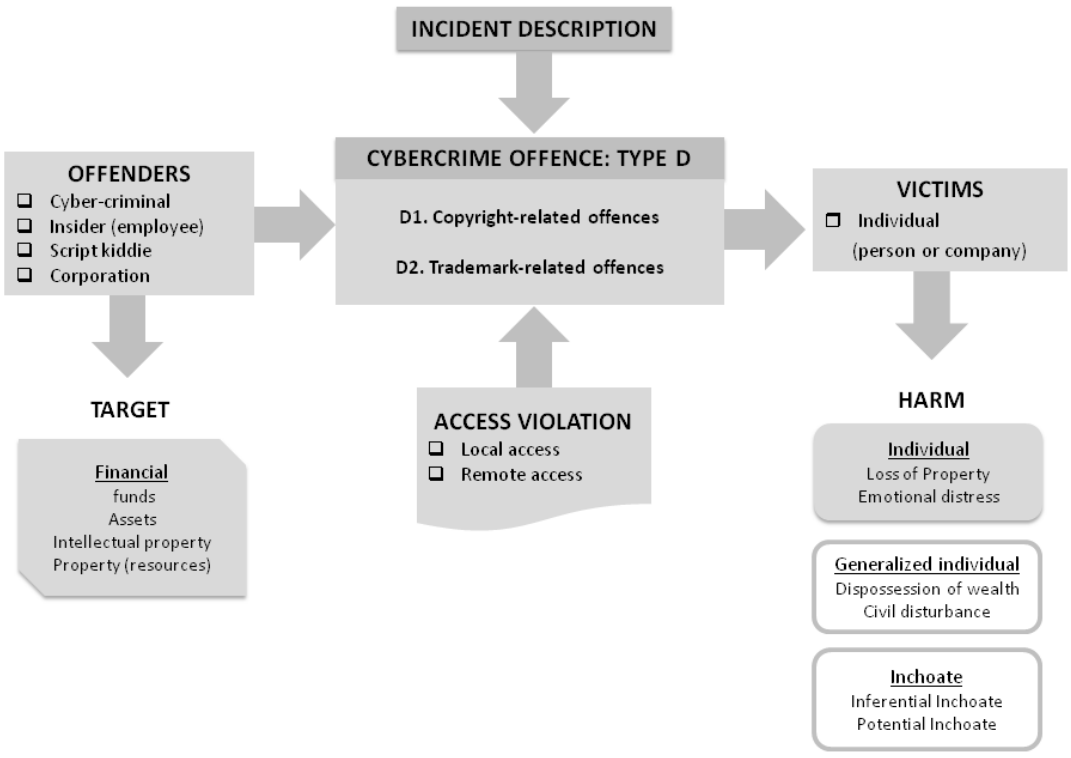

Figure 4. Incident description schema for type D offences

These offences are committed by cybercriminals, insiders (employees), script kiddies or corporations, while victims are either the creators or right holders of the intellectual property. The purposes of those conducting the crimes are exclusively financial, because illegal distribution of data characterized as intellectual property is highly profitable. What has to be mentioned is that despite being illegal, authors do not include personal viewing as a target of cybercriminals due to the fact that the inflicted harm to the ones holding intellectual property is barely noticeable in isolated incidents. When the infringements though become great in number and a specific user is the one responsible, it is highly possible that his purpose is financial exploitation for gaining profit. As for the inflicted harm, this is likewise orientated to losses of property for the individual, person or entity, targeted and correspondingly emotional distress. In regards to society, generalized harm is about dispossession of wealth from victims to offenders and civil disturbance in large-scale incidents. The potential inchoate harm is in this offence type extremely possible, as data distributed through the web cannot be tracked and therefore in foreseeable future, losses in property will continue.

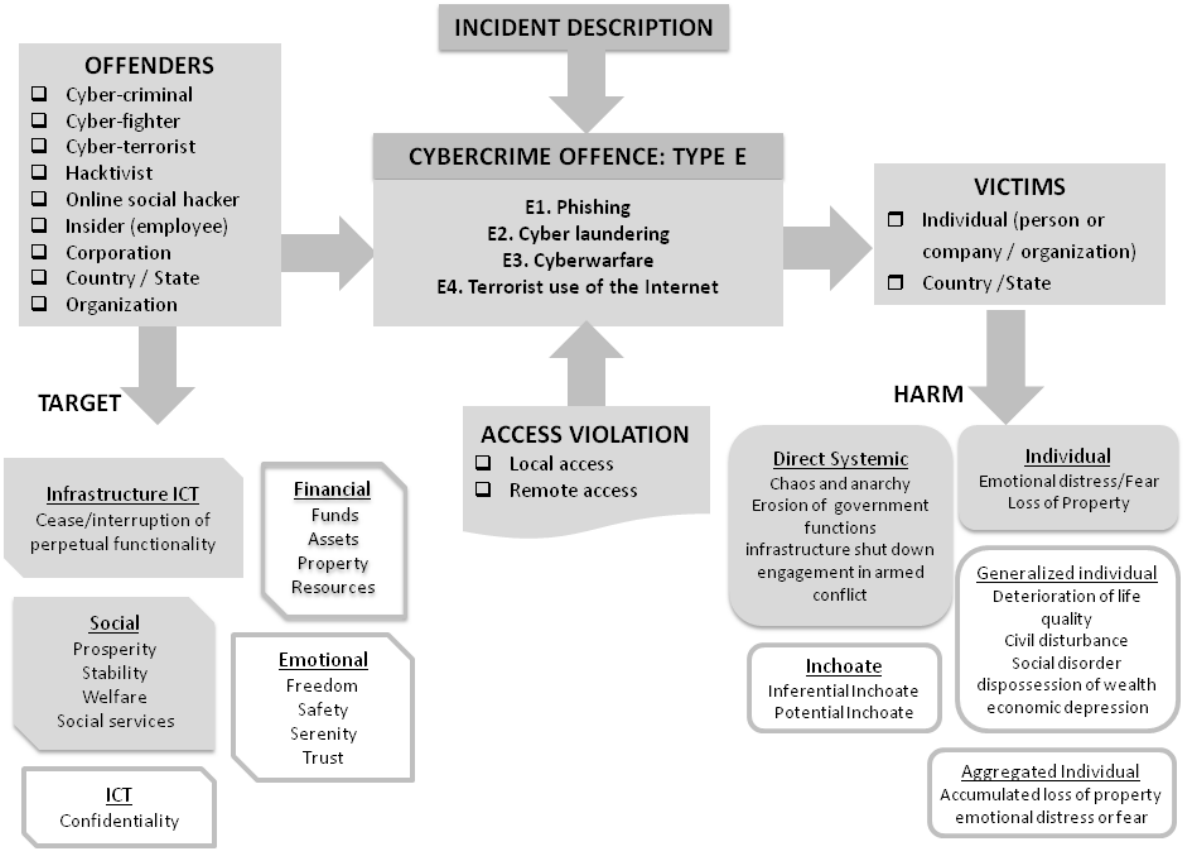

Figure 5. Incident description schema for type E offences

In this offence type are encompassed cybercrimes with combinational characteristics and therefore do not share many commonalities in nature. The possible offenders are virtually every one described in the corresponding chapter as especially terrorist use of internet and cyberwarfare are large scale incidents that last in time and involve many participants with different orders but same target and methodology. In these offences infrastructure ICT are initially targeted in order to cease/interrupt perpetual functionality and also society by afflicting prosperity, stability, and generally welfare. The purposes of terrorists are also emotional abuse of the targeted country's civilians by afflicting freedom, safety and serenity. The harm caused is initially direct systemic and can vary from infrastructure shut down, erosion of government functions, chaos and anarchy, to engagement of the country to armed conflict.

The generalized individual harm includes the deterioration of life quality, social disorder and economic depression while the potential inchoate harm is in respect to how soon a society can overwhelm a traumatic experience e.g. a terrorist attack. Regarding the other offences of this category, the offender's target is either ICT abuse of confidentiality for phishing attacks or financial abuse of assets, funds and property for both cyberlaundering and phishing. The harm is individual due to the corresponding loss of property, aggregated individual harm when phishing attacks are in form of spam and inchoate potential harm from the illegally acquired personal information. Lastly, cyberlaundering can inflict individual harm in the form of property loss to the country these transactions took place, and generalized harm as economic depression of society in extreme situations.

5. Discussion and Conclusions

The authors identified and presented the features of cybercrime incidents, a classification system for related offences and a schema that binds together the various elements and examines their interrelations to better suggest corresponding actions, measures and policies. The process involved revision of reports conducted by authorities, academia and agencies related to information security. The identification of cybercrime features allows for a more comprehensive description of individual incidents that leads to better understanding, handling and management of their occurrences. The modular feature-based approach towards description of incidents allows for additional features to be included in the future.

Also the expansion or consolidation of their respective elements can also be achieved depending on specific perspectives.

The paper also proposed a comprehensive two-level classification system of cybercrime offences based on European Union's initial typology and further analysis taking account of the present status and recent forms of cybercrime. The system encompasses the most common forms of computer-related offences and can prove useful in Law Enforcement agencies. Furthermore, the proposed system is included as part of the feature-based description to classify a cybercrime incident under a corresponding criminal offence. The overview (table 7) of the identified cybercrime features and their respective elements provided the opportunity of examining possible dependencies and interrelations based on the generic type (level-1) of the corresponding offence. This was assisted through a schema-based depiction of the specific features and elements for each type (figures 1 to 5).

The end result is an approach towards describing cybercrime incidents utilizing a systematic approach that can lead to: (a) better understanding of the specific incidents, (b) accurate monitoring and grouping of similar occurrences and (c) better investigation of the specific elements involved in each respective case. The schema can evolve following the development of information technologies, either to encompass new elements in each feature, i.e. when a new cybercrime offence appears, or to alter the way elements are connected with each other, as offenders constantly conceive new ways to have the desired effect. There is also ongoing research by the authors to introduce a new feature in the schema, regarding specific actions, counter measures and policies based on the offence type, and taking into consideration the incident occurrence frequency. The severity, urgency and typical characteristics of the identified cybercrimes, require different preventive measures towards mitigation, while the same applies for the actions needed during crime conduction, and policies implemented in national or international level. The addition and implementation of such feature will highlight the importance of not only understanding the problem but also proposing suitable and effective solutions towards it. By emulating the decision-making ability of a human expert, the lack of communication and mutual understanding between agencies that hinders mutual progress can significantly improve.

A future extension could take into account the frequency of occurrences in order to propose custom actions, measures and policies, and finally incorporate the

produced schema in an automated incident management system with standard operating procedures and protocols. The operational efficiency of such system would provide automated identification of incidents and emergency response protocols. Furthermore, all information handled by the system would be recorded to produce analytics and visualizations for gaining insights and future planning, leading to optimization of handling cybercrime incidents.

References

[1] D. L. Shinder and M. Cross, *Scene of the Cybercrime*. Syngress, 2008.

[2] FBI and NW3C, "2014 Internet Crime Report," 22-May-2015. [Online]. Available: https://pdf.ic3.gov/2014_IC3Report.pdf. [Accessed: 17-May-2016].

[3] FBI and NW3C, "IFCC 2002 Internet Fraud Report," 2003.

[4] PricewaterhouseCoopers, "The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world," 30-Sep-2014. [Online]. Available: http://www.pwccn.com/webmedia/doc/635527689739110925_rcs_info_security_2015.pdf. [Accessed: 19-May-2016].

[5] Federal Criminal Police Office, "Police Crime Statistics 2008," 2009. [Online]. Available: http://www.bka.de/nn_194638/sid_73974E4F691258D85603C3F55F3BCC72/SharedDocs/Downloads/EN/Publications/PoliceCrimeStatistics/2002Bis2013/pks2008_englisch.html?__nnn=true. [Accessed: 18-May-2016].

[6] PricewaterhouseCoopers, "2015 US State of Cybercrime Survey," *PwC*, Jul-2015. [Online]. Available: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.html. [Accessed: 18-May-2016].

[7] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The economics of information security and privacy*, Springer, 2013, pp. 265–300.

[8] L. D. Roberts, *Cyber-victimisation in Australia: Extent, impact on individuals and responses*. Tasmanian Institute of Law Enforcement Studies, 2008.

[9] K. M. Finklea and C. A. Theohary, "Cybercrime: conceptual issues for congress and US law enforcement," 2012.

[10] Council of Europe, "Convention on Cybercrime," 23-Nov-2001. [Online]. Available: http://www.coe.int/el/web/conventions/full-list/-/conventions/treaty/185. [Accessed: 27-Apr-2016].

[11] Council of Europe, "Summary to the Convention on Cybercrime (ETS N° 185)," *Treaty Office*, 23-Nov-2001. [Online]. Available: http://www.coe.int/web/conventions/full-list. [Accessed: 18-Dec-2015].

[12] Council of Europe, "Explanatory Report to the Convention on Cybercrime (ETS N° 185)," *Treaty Office*, 23-Nov-2001. [Online]. Available: http://www.coe.int/web/conventions/full-list. [Accessed: 18-Dec-2015].
[13] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in Computer Virology*, vol. 2, no. 1, pp. 13–20, 2006.
[14] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.
[15] I. Walden, *Computer crimes and digital investigations*. Oxford University Press, Inc., 2007.
[16] M. E. Kabay, "Understanding Studies and surveys of computer Crime," *Computer Security Handbook*, 2009.
[17] L. Marinos, A. Belmonte, and E. Rekleitis, "ENISA Threat Landscape 2015," 27-Jan-2016. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015. [Accessed: 31-Mar-2016].
[18] A. Tsesis, "Hate in cyberspace: Regulating hate speech on the Internet," *San Diego L. Rev.*, vol. 38, p. 817, 2001.
[19] National Crime Prevention Council and Office for Victims of Crime, "Cyberbullying — National Crime Prevention Council," 2009. [Online]. Available: http://www.ncpc.org/topics/cyberbullying. [Accessed: 21-Apr-2016].
[20] Warwick Ashford, "Service model driving cyber crime, says Europol report," *ComputerWeekly*, 29-Sep-2014. [Online]. Available: http://www.computerweekly.com/news/2240231663/Service-model-driving-cyber-crime-says-Europol-report. [Accessed: 21-Apr-2016].
[21] C. Hargreaves and D. Prince, "Understanding cyber criminals and measuring their future activity," 2013.
[22] R. Stone, "A Call to Cyber Arms," *Science*, vol. 339, no. 6123, pp. 1026–1027, Mar. 2013.
[23] P. Wu, "Impossible to Regulate: Social Media, Terrorists, and the Role for the UN," *Chi. J. Int'l L.*, vol. 16, p. 281, 2015.
[24] A. Brill and L. Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?," *Defence Against Terrorism Review*, vol. 6, no. 1, 2014.
[25] P. A. Taylor, "From hackers to hacktivists: speed bumps on the global superhighway?," *New Media & Society*, vol. 7, no. 5, pp. 625–646, 2005.
[26] Verizon, "Data Breach Investigations Report," *Verizon Enterprise Solutions*, 2014. [Online]. Available: http://www.verizonenterprise.com/DBIR/2014/. [Accessed: 21-Apr-2016].
[27] PricewaterhouseCoopers, "The Global State of Information Security Survey," *PwC*, 2016. [Online]. Available: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html. [Accessed: 21-Apr-2016].

[28] L. Marinos, "ENISA Threat Landscape 2013," 11-Dec-2013. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats. [Accessed: 31-Mar-2016].

[29] J. McDermott and C. Fox, "Using abuse case models for security requirements analysis," in *Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual*, 1999, pp. 55–64.

[30] D. Riley, "15-year-old script kiddie arrested in TalkTalk hacking investigation," *SiliconANGLE*, 27-Oct-2015. .

[31] B. H. Schell, M. V. Martin, P. C.K. Hung, and L. Rueda, "Cyber Child Pornography: a Review Paper of the Social and Legal Issues and Remedies-and a Proposed Technological Solution," *Aggression and Violent Behavior*, vol. 12, no. 1, pp. 45–63, 2007.

[32] M. Balfe, B. Gallagher, H. Masson, S. Balfe, R. Brugha, and S. Hackett, "Internet child sex offenders' concerns about online security and their use of identity protection technologies: a review," *Child Abuse Review*, vol. 24, no. 6, pp. 427–439, 2015.

[33] K. J. Higgins, "Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm," *Dark Reading*, 10-Feb-2015. [Online]. Available: http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025. [Accessed: 19-May-2016].

[34] K. J. Biba, "Integrity considerations for secure computer systems," DTIC Document, 1977.

[35] M. G. Leary, "Self-produced child pornography: The appropriate societal response to juvenile self-sexual exploitation," *Va. J. Soc. Pol'y & L.*, vol. 15, p. 1, 2007.

[36] S. W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?," *Va. JL & Tech.*, vol. 9, pp. 13–13, 2004.

[37] S. W. Brenner, "Complicit publication: When should the dissemination of ideas and data be criminalized," *Albany Law Journal of Science & Technology*, vol. 13, no. 2, 2003.

[38] M. Gercke, "Understanding cybercrime: Phenomena, challenges and legal response," ITU, Sep. 2012.

[39] European Committee on Crime Problems and Council of Europe Directorate of Legal Affairs, *Computer-related crime: recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*. Council of Europe, 1989.

[40] U.S House of Representatives, "18 U.S. Code § 1030 - Fraud and related activity in connection with computers," *LII / Legal Information Institute*, 1986. [Online]. Available: https://www.law.cornell.edu/uscode/text/18/1030. [Accessed: 27-May-2016].

[41] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, P. Gill, and R. J. Deibert, "Targeted threat index: Characterizing and quantifying politically-motivated targeted malware," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 527–541.

[42] B. Binde, R. McRee, and T. J. O'Connor, "Assessing outbound traffic to uncover advanced persistent threat," *SANS Institute. Whitepaper*, 2011.

[43] N. Virvilis, D. Gritzalis, and T. Apostolopoulos, "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?," in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 2013, pp. 396–403.

[44] Office of the UN High Commissioner for Human Rights (OHCHR), UN Office on Drugs and Crime (UNODC), and Irish Centre for Human Rights (ICHR), *Model Codes for Post-Conflict Criminal Justice*. United States Institute of Peace, 2007.

[45] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy of computer worms," in *Proceedings of the 2003 ACM workshop on Rapid malcode*, 2003, pp. 11–18.

[46] Council of Europe, "Details of Treaty No.185," *Treaty Office*, 23-Nov-2001. [Online]. Available: http://www.coe.int/web/conventions/full-list. [Accessed: 15-Mar-2016].

[47] O. SSA, "Title 18 United States Code," 07-Jan-2011. [Online]. Available: https://www.ssa.gov/OP_Home/comp2/D-USC-18.html. [Accessed: 15-Mar-2016].

[48] K. M. Dolan, "Internet auction fraud: the silent victims," *Journal of Economic Crime Management*, vol. 2, no. 1, pp. 1–22, 2004.

[49] E. Finch, "What a tangled web we weave: Identity theft and the internet," *Dot. cons: Crime, Deviance, and Identity on the Internet. Cullompton, England: Willan*, 2003.

[50] Council of Europe, *Parliamentary Assembly Documents 2001 Ordinary Session (Second Part), Volume V*. Council of Europe, 2001.

[51] F. Paget, "Identity theft," *McAfee Avert Labs technical white paper No*, vol. 1, 2007.

[52] M. Gercke, "Internet-Related Identity Theft," *Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France*, 2007.

[53] D. J. Harris, M. O'Boyle, E. Bates, and C. Buckley, *Harris, O'Boyle, and Warbrick Law of the European Convention on Human Rights*. Oxford University Press, 2014.

[54] J.-F. Renucci, *Introduction to the European Convention on Human Rights: The Rights Guaranteed and the Protection Mechanism*. Council of Europe, 2005.

[55] United Nations High Commissioner for Refugees, "Refworld | The Johannesburg Principles on National Security, Freedom of Expression and

Access to Information," *Refworld*, 01-Oct-1995. [Online]. Available: http://www.refworld.org/docid/4653faif2.html. [Accessed: 03-Mar-2016].
[56] J. Ropelato, *Internet pornography statistics*. 2006.
[57] S. Livingstone and M. Bober, "UK Children Go Online: Surveying the experiences of young people and their parents," 2004.
[58] Michael C Seto, Chantal A. Hermann, Cecilia Kjellgren, Gisela Priebe, Carl Go ¨ran Svedin, and Niklas La ˚ngstro ¨m, "Viewing Child Pornography: Prevalence and Correlates in a Representative Community Sample of Young Swedish Men," *Archives of sexual behavior*, vol. 44, no. 1, 2014.
[59] K. M. Babchishin, R. K. Hanson, and H. VanZuylen, "Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children," *Archives of sexual behavior*, vol. 44, no. 1, pp. 45–66, 2015.
[60] M. Franek, "Foiling cyberbullies in the new wild west," *Educational Leadership*, vol. 63, no. 4, p. 39, 2005.
[61] R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and M. R. Lattanner, "Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth.," *Psychological bulletin*, vol. 140, no. 4, p. 1073, 2014.
[62] N. von Marées and F. Petermann, "Cyberbullying: An increasing challenge for schools," *School Psychology International*, vol. 33, no. 5, pp. 467–476, 2012.
[63] F. Sticca and S. Perren, "Is cyberbullying worse than traditional bullying? Examining the differential roles of medium, publicity, and anonymity for the perceived severity of bullying," *Journal of youth and adolescence*, vol. 42, no. 5, pp. 739–750, 2013.
[64] S. Schneider, "Towards a Comprehensive European Framework on Online Gaming," *Gaming Law Review and Economics*, vol. 17, no. 1, pp. 6–7, 2013.
[65] European Commission, "Communication from the Commission to the European Parliament, the Council, the economic and social Committee and the Committee of the Regions 'Towards a comprehensive European framework for online gambling'.," 2012. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0596&from=EN. [Accessed: 09-Mar-2016].
[66] Messaging Anti-Abuse Working Group and others, *Email Metrics Program: The Network Operator's Perspective. Report 14*. 2011.
[67] Marc Rotenberg and Samantha Liskow, "Consumer perspectives on spam: Challenges and challenges," presented at the ITU World Summit on the Information Society (WSIS) thematic meeting on Countering Spam, Geneva, 2004.
[68] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," *Artificial Intelligence Review*, vol. 29, no. 1, pp. 63–92, 2008.

[69] Simon Wiesenthal Center, "Digital Terrorism and Hate 2007. Growing Menace of Digital Terrorism and Hate Exposed in New SWC Interactive Report," *Pressemitteilung vom*, vol. 7, p. 2007, 2007.
[70] N. Van Eijk, P. Rutten, and J. Poort, "Legal, economic and cultural aspects of file sharing," *Communications & Strategies*, no. 77, pp. 35–54, 2010.
[71] A. Huygen, N. Helberger, J. Poort, P. Rutten, and N. Van Eijk, "Ups and downs; economic and cultural effects of file sharing on music, film and games," *TNO Information and Communication Technology Series*, 2009.
[72] F. Oberholzer-Gee and K. Strumpf, "The effect of file sharing on record sales: An empirical analysis," *Journal of political economy*, vol. 115, no. 1, pp. 1–42, 2007.
[73] S. Androutsellis-Theotokis and D. Spinellis, "A survey of peer-to-peer content distribution technologies," *ACM computing surveys (CSUR)*, vol. 36, no. 4, pp. 335–371, 2004.
[74] T. J. Curtin, "Name Game: Cybersquatting and Trademark Infringement on Social Media Websites, The," *JL & Pol'y*, vol. 19, p. 353, 2010.
[75] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.
[76] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.
[77] W. Filipkowski, "Cyber laundering: an analysis of typology and techniques," *International Journal of Criminal Justice Sciences*, vol. 3, no. 1, p. 15, 2008.
[78] N. Cohen, "Speed Bumps on the Road to Virtual Cash," *The New York Times*, 03-Jul-2011.
[79] Coalition for International Justice, "Following the money 101: A primer on money-trail investigations," Feb. 2004.
[80] R. C. Molander, A. Riddile, and P. A. Wilson, "Strategic Information Warfare," 1996. [Online]. Available: http://www.rand.org/pubs/monograph_reports/MR661.html. [Accessed: 27-Mar-2016].
[81] Matt Murphy, "War in the fifth domain," *The Economist*, 01-Jul-2010.
[82] A. Bright, "Estonia accuses Russia of 'cyberattack,'" *Christian Science Monitor*, 17-May-2007.
[83] Eneken Tikk, Kadri Kaska, and Lils Vihul, "International Cyber Incidents: Legal Considerations," *CCDCOE*, 16-Sep-2014. [Online]. Available: https://www.ccdcoe.org/multimedia/international-cyber-incidents-legal-considerations. [Accessed: 27-Mar-2016].
[84] P. C. Reich, S. Weinstein, C. Wild, and A. S. Cabanlong, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity," *European Journal of Law and Technology*, vol. 1, no. 2, Oct. 2010.
[85] T. L. Thomas, "Al Qaeda and the Internet: The danger of' cyberplanning,'" *Parameters*, vol. 33, no. 1, p. 112, 2003.
[86] M. Conway, "TerroristUse'of the Internet and Fighting Back," *Information and Security*, vol. 19, p. 9, 2006.

[87] W. Krzysztof, "Money laundering techniques with electronic payment systems," *International&Security. An International Journal*, pp. 27–47, 2006.
[88] W. J. Clinton, "Executive order 13010-critical infrastructure protection," *Federal Register*, vol. 61, no. 138, pp. 37347–37350, 1996.