Cybercrime Offences: Identification, Classification and Adaptive Response

George Tsakalidis, Graduate Student Member, IEEE, Kostas Vergidis and Michael Madas

Abstract— **Multiple studies and surveys focus on specific cybercrime characteristics or develop classification models that do not adequately address the complexity of this contemporary type of crime. This study proposes a comprehensive approach towards cybercrime interpretation and action recommendation through a proposed framework that provides three separate and complementary views to achieve a comprehensive perspective that leads to actionable recommendations. The framework's view I identifies the features of a cybercrime incident and their corresponding elements generating a textual schema-based description that can accommodate existing and new instances of cybercrime. The second view introduces an up-to-date cybercrime-related offence classification system through consolidation and elaboration of existing approaches and leads to a visual extension of schema-based incident description that depicts the interrelations of the various cybercrime elements towards a particular type of offence. View III identifies and interconnects the relevant stakeholders with preventive and response actions and measures. The proposed framework extends previous published work on the theoretical foundation of this multi-faceted domain, and demonstrates that the necessity of a comprehensive approach towards cybercrime can be actualized through different steps with each one designated towards a different perspective.**

I. Introduction

Due to the dynamic and continuously evolving nature of new types of electronic crime, the term cybercrime has come to encompass a variety of criminal offenses, and consequently its definition still relies heavily on the perspective of the stakeholder. During the last decades a lot of research has been conducted aiming to a conclusive and comprehensive typology for cybercrime-related offenses. A classification, was recommended by [1] proposing three distinct categories: (a) Computer Integrity Crimes and specifically the illegal activities of cracking, hacking and denial of service, (b) Computer-Assisted Crimes are the offences of virtual robberies, scams and theft, and (c) Computer Content Crimes that include pornography, violence and offensive communications.

An extensive and up-to-date classification systems is the ENISA threat taxonomy [2] conducted by the European Union Agency for Network and Information Security (ENISA). A considerable gap though is apparent, due to the fact that ENISA categorizes threats to cybersecurity instead of cybercrimes in general, excluding offences related to illegal content. An inclusive classification system was proposed by EUROPOL's European Cybercrime Centre (EC3) [2], classifying incidents along two vectors, type of incident and type of event for the categorization to be grouped on the basis of the lowest common denominator. Despite the categorization efforts, there is still none acceptable and comprehensive system for universal classification of the various cybercrime-related offences. As it is extensively documented in [3], three of the main challenges that prohibit effective classification, measure recommendation and overall handling of cybercrime-related offences are:

1. The lack of a unanimous understanding for the technology-induced types of offences,
2. Deficiency in the conception of a widely accepted classification system for the various,
3. The absence of a set of complementary appropriate measures and effective policies for each offense incidents.

To address the above, this paper proposes a framework for Identification, Classification and Adaptive Response (ICAR) to Cybercrime-related Offences (ICAR), which incorporates three distinct views as shown in Table I. A cybercrime has multiple features that describe each unique characteristic, and they have to be identified for optimal interpretation (view I). This procedure can produce a detailed definition for every identified cybercrime incident, the variety of which necessitates their assemblage in a comprehensive offence classification system (view II). The identified features and classification of offences, as introduced in views I and II, have been previously published by the authors in [3], lacking though a countering perspective which is essential for the actual application of knowledge by the involved stakeholders. This research gap is addressed through ICAR view III which provides preventive measures, tackling actions and policies combining law, directives and mitigation recommendations matching with particular incidents and offence types. The ICAR framework encompasses the crucial characteristics for the formulation of effective regulatory and legal frameworks, as in [4].

II. Feature identification of cybercrime incidents

The first view of the framework deals with identifying the features that distinguish cybercrime-related incidents. The

G. Tsakalidis is with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki 54 636, Greece (e-mail: giorgos.tsakalidis@uom.edu.gr).

K. Vergidis is with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki 54 636, Greece (corresponding author to provide phone: 2310-891637; e-mail: kvergidis@uom.gr).

M. Madas is with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki 54 636, Greece (e-mail: mmadas@uom.gr).

issues with providing a detailed description about cybercrime incidents are: (a) there is already an adversity in existing cybercrime definitions, and (b) the incidents classified as cybercrime demonstrate a significant variety in their features and characteristics. 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: (i) a better understanding of a specific incident, (ii) accurate classification of the corresponding criminal offence and (iii) assignment of effective action in terms of prevention, incident response and policy generation.

TABLE I. OVERVIEW OF THE ICAR FRAMEWORK

ICAR Views	Motivation	Proposed Approach	Outcome / Contributions
view I	Lack of detailed description of incidents.	Cybercrime schema-based description and identification of incident features.	Clarifies whether a criminal activity is a cybercrime and provides a detailed mechanism for describing incidents
view II	Lack of a unanimous classification system in existing approaches.	Typology is based on CoC's (2001) and Gercke's (2012) classification, with five general categories and the corresponding offences.	Introduces an extensive classification system that enables analysis and monitoring of similar offences, and allows correlation /addition of future and new offence types.
view III	Communication adversities between agencies and lack of centralized counteract approach.	Aggregation of appropriate actions and measures and visual representation of the temporal interconnection of stakeholders to the measures.	Assignment of selected actions and measures to offences, for prevention and countering depending on circumstances.

The first step towards this schema is to determine the basic features of a cybercrime incident. Table II presents seven identified features that describe an incident in a comprehensive way. Each identified feature 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 a movie file). The second feature (identified offence) answers to the question on whether this particular incident is considered criminal activity and under which criminal offence to be classified.

The third feature (offender) specifies the individual or entity responsible for the offence committed, whereas the fourth feature (access violation) is unique to cybercrime offences as it highlights the way 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. The next step is to identify the various elements of each feature to accurately describe a cybercrime-related incident and further examine any possible interrelations between elements that would highlight specific aspects of cybercrime offences.

TABLE II IDENTIFIED FEATURES OF CYBERCRIME INCIDENTS

no.	feature	feature description	answers the question
1	INCIDENT	description of the incident	What happened?
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?

The identified features and their particular elements have been described in detail in [3] and help produce a comprehensive textual schema-based incident description that combines the identified features:

> 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].

A cybercrime incident thus could be described based on the proposed contextualization as follows: *The non-delivery of merchandize regarding an online purchase [incident] is the offence of computer-related fraud [identified offence], committed by a cyber-criminal [offender], conducted through internet [access violation] against the property, serenity, trust and mentality [target] of an individual [victim], resulting in loss of property, moral harm, emotional distress and inferential inchoate harm [harm].* It is evident that a specific incident and its impact are accurately depicted when the specific elements of its features are detailed. Moreover, this approach allows the examination of possible dependencies between the various elements, that provide a more eloquent perspective on particular cybercrime offences.

III. OFFENCE CLASSIFICATION SYSTEM

The proposed offence classification system is based on two layers: The first layer consists of the four different types (A, B, C, D) of cybercrime offences introduced in the Convention on Cybercrime [7] with the authors' addition of a new type (E): the combinational offences. Three offence types (A, C, D) focus on the object of legal protection, type B focuses on the method used to commit the crime and type E that describes offences with complex interface not falling under any of the previous types. For each layer-1 offence type, there are layer-2 sub-categories based on Gercke, "Understanding Cybercrime: Phenomena, Challenges and Legal Response." [6]. The authors updated layer-2 sub-categories in [6] to provide a contemporary and consistent classification system. The offence "misuse of devices" is transferred from Type B category to type A, because it may require a computer system to occur which is the main characteristic of this offence type, but the exclusive motive of the misuse is unauthorized access and illegitimate tampering. The authors also introduce cyberbullying under type C offences, as it was not included in [6]. This type of offence is linked to the rise of social media and as technology advances so are the diverse applications and typologies of cyberbullying. The authors omitted the offence of "libel and false information" as the more severe incidents can be classified under the offence of "racism and hate speech on the Internet" and "cyberbullying," e.g., in defamation. Regarding the offense of dissemination of false information with no potential impact, the authors consider it difficult to incriminate thus not necessary to fall under a discrete subcategory. Lastly, Gercke [6] included the offence "other forms of illegal content" under the category content-related offences that is considered redundant due to the resemblance with other offences in the proposed classification. For example, providing information and instructions for illegal acts (e.g., how to build explosives) falls under the offense of "terrorist use of the Internet."

The set of five generic categories of the proposed classification is briefly presented as follows:

Type A - Offences against the confidentiality, integrity and availability of computer data and systems. This type includes the core of computer-related offences, offences representing the major threats, as identified in the discussions on computer and data security to which electronic data processing and communicating systems are exposed [8]. The types of crime covered are mostly unauthorized access and illicit tampering with systems, programs or data:

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. 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. As computer-related offences, authors classify:

B1. Computer-related forgery
B2. Computer-related fraud
B3. Identity theft

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. It should be noted that a national approach can, in fact, interfere with the legal system of another country. Taking into account what is considered legitimate in most countries, the authors introduce the following illegal activities:

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. Copyright infringements are one of the most widespread forms of computer-related crime and its escalation is causing international concern. Intellectual property (e.g. media files and products) can be downloaded, copied and distributed, and therefore is subject to counterfeiting and copyright violations in general. These offences are:

D1. Copyright-related offences
D2. Trademark-related offences

Type E - Combinational offences. The last category includes combination of offences that have already been mentioned in the four previous types. Due to increasing Law Enforcement collaboration and public concern-alert, offenders improvise and progress their methods in order to maintain their effectiveness. The most representative and common combinational offences are:

E1. Phishing
E2. Cyber laundering
E3. Cyberwarfare
E4. Terrorist use of the Internet

The accurate and effective identification of cybercrime incidents necessitates the analysis and interpretation of cybercrime features and their corresponding elements along with the possible interrelations between them [3]. Toward this direction, the authors propose a comprehensive visual schema-based incident description that combines the identified features. The outcome of ICAR view II is the visual extension of the textual schema-based cybercrime incident description. The schema is organized around the types of offences as different elements of the identified features are more prominent. In Figure 1 the authors present the interrelation of features for type A offences. These 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.

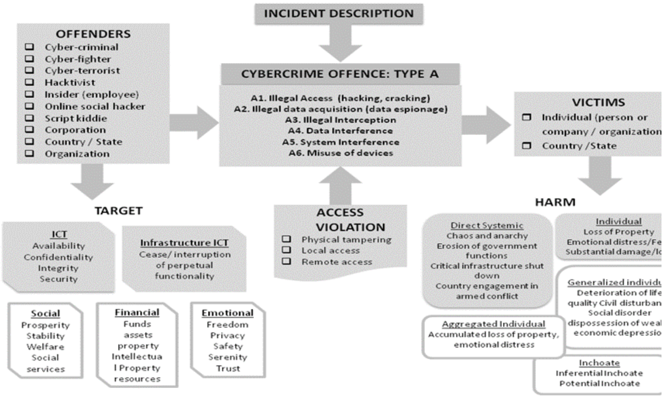


Figure 1. Incident description visual schema for type A offences

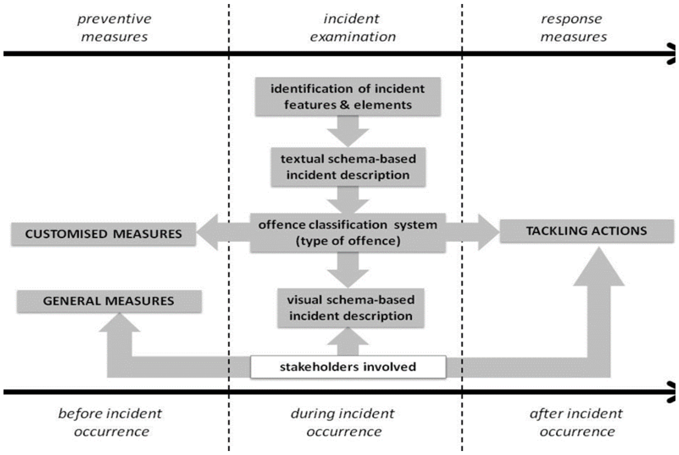

preventive measures
incident examination
response measures
identification of incident features & elements
textual schema-based incident description
CUSTOMISED MEASURES
offence classification system (type of offence)
TACKLING ACTIONS
GENERAL MEASURES
visual schema-based incident description
stakeholders involved
before incident occurrence
during incident occurrence
after incident occurrence

Figure 2. Preventive and response measures in relation to incident occurrence

IV. RECOMMENDATION OF ACTIONS, MEASURES & POLICIES

The third view of the ICAR framework is related to: (a) immediate actions to handle cybercrime incidents, (b) specific measures to prevent similar offences and (c) elaborate policies that suggest formal action towards a specific category of cybercrime. A separation of these acts is essential, mostly regarding time of implementation as there are preventive measures and policies that precede response and tackling actions. View III introduces three features in relation to tackling cybercrime:

- The stakeholders of policies, measures and actions,
- The preventive measures and policies, and
- The response measures and tackling actions.

Figure 2 demonstrates how the preventive and response measures are connected in relation to a cybercrime incident occurrence. Regarding the time before incident, the authors propose general preventive measures in form of good practices by all involved stakeholders and measures customized to the cybercrime types. During the incident, ICAR Framework identifies the elements of each feature, provides a textual schema-based description and a visual descriptive extension of the incident type.

As for the last stage, specific tackling actions for each type are appointed to the stakeholders with immediate reporting to national law enforcement agency. The measures necessary for cybercrime prevention are divided to: (a) typical preventive measures forming the core of cybercrime prevention that aims to cybercrime mitigation in general, and (b) sets of measures with customized methodology for the specific cybercrime offense types.

A. *Stakeholders*

This element encompasses all parties involved with tackling cybercrime incidents or preventing them.

1) *Governments*

The need for a national cybercrime strategy, prompts governments to frame responses regarding prevention laws and policies. Their role also requires assignment of duties and responsibilities for involved institutions and agencies, along with proper organization and coordination of legal frameworks.

2) *Private and public sector organizations and institutions*

Private and public sector organizations play a vital role against Cybercrime. Good practices and cybercrime incident management adopted by organizations, along with the establishment of successful public-private cybersecurity partnerships are necessary to prevent and address the evolving landscape.

3) *Internet service and hosting Providers*

Internet service and hosting providers control the systems upon which internet services run and amongst others, monitor, filter internet traffic and track illegal use of devices. They have been assigned with critical responsibilities, obligations and jurisdictions, in collaboration with enforcement agencies.

4) *National and cross national law enforcement agencies*

Law enforcement agencies are responsible for recording, investigating and finally tackling IT crimes committed within their territories. Due to the transnational nature of cybercrime, agencies develop cooperation mechanisms and procedures.

5) *Academic institutions*

Academic institutions also contribute towards cybercrime prevention, in particular, through development of appropriate legislation and policies, development in technical standards and technology, knowledge sharing [9] and public awareness raising.

6) *Users*

The actual victims of cybercrime incidents are individual users, that highlights the importance of taking measures through adopting good practices in ICT usage.

B. General preventive measures and policies

The typical measures towards cybercrime prevention are matched to the stakeholders that should apply them.

1) Governments

- Promulgation of appropriate legislation [10], and regular revision in accordance with international standards.
- Establishment of national cybersecurity strategy.
- Participation in international cooperation for the development of cybercrime legal frameworks.

2) Private – Public sector organizations and institutions

- Continuous training of employees on cybersecurity awareness and safe use of ICT devices.
- Management of individual authentication and authorization, along with the provided privileges within or across system and enterprise boundaries [11].
- Backing up of technical controls by operational controls such as continuous firewall rule reviews and on-going verification of these rules [12].

3) Internet service and hosting Providers

- Data retention by ISPs regarding specific customer online activities for time periods, during which agencies can investigate with the required judicial authorization.
- ISPs are tasked with compulsory data breach notification when personal data is disclosed or illegally acquired.
- ISP's Protection from intermediary liability can provide the initiative for suitable actions following the incidents.

4) National and cross-national law enforcement agencies

- Proper evaluation of computer security risks and remedies.
- Efficient role assignment and analytical procedures and investigation techniques.
- Utilization of civil resources to enhance striking power, efficacy and accuracy of their work [13].

5) Academia

- Academic institutions foster knowledge development and sharing through educational programs, curricula and research centers.
- Academics provide legal advice and assist legislative bodies on topics such as criminalization and legal protection.
- Provision of technical assistance to law enforcement, corporations and finally individual users [14].

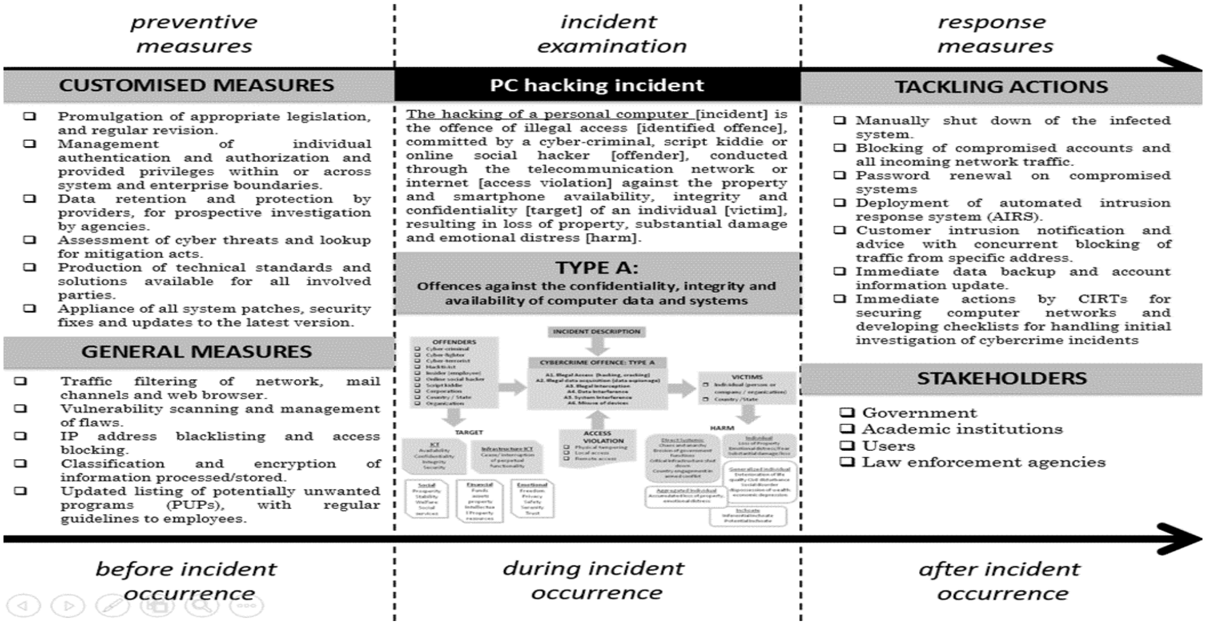
6) Users

- Appliance of all published system patches, security fixes and updates[15].
- Regular password renewal with balance between usability and security [16].
- Backups and encryption of personal information through proper encryption software.

C. Customized preventive measures and policies

This section introduces preventive measures customized to type A based on the proposed classification system (view II). Measures for the remaining types can be produced accordingly.

- Proper classification of information processed or stored and subsequent encryption for different levels of privacy.
- Categorization of data regarding importance and protection necessity.
- Direct control of all portable devices accessing a business network by administrators, to avoid pod slurping [11].



❑ Promulgation of appropriate legislation, and regular revision.
❑ Management of individual authentication and authorization and provided privileges within or across system and enterprise boundaries.
❑ Data retention and protection by providers, for prospective investigation by agencies.
❑ Assessment of cyber threats and lookup for mitigation acts.
❑ Production of technical standards and solutions available for all involved parties.
❑ Appliance of all system patches, security fixes and updates to the latest version.

❑ Traffic filtering of network, mail channels and web browser.
❑ Vulnerability scanning and management of flaws.
❑ IP address blacklisting and access blocking.
❑ Classification and encryption of information processed/stored.
❑ Updated listing of potentially unwanted programs (PUPs), with regular guidelines to employees.

The hacking of a personal computer [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].

❑ Manually shut down of the infected system.
❑ Blocking of compromised accounts and all incoming network traffic.
❑ Password renewal on compromised systems
❑ Deployment of automated intrusion response system (AIRS).
❑ Customer intrusion notification and advice with concurrent blocking of traffic from specific address.
❑ Immediate data backup and account information update.
❑ Immediate actions by CIRTs for securing computer networks and developing checklists for handling initial investigation of cybercrime incidents

❑ Government
❑ Academic institutions
❑ Users
❑ Law enforcement agencies

Figure 3. Preventive and response measures in relation to incident occurrence

- Application of whitelisting for rogue software to be blocked, and IP address blacklisting and consequent access blocking.
- Updated listing of potentially unwanted programs (PUPs), with regular guidelines to employees for avoiding installation.

D. Response measures and tackling actions

This section introduces a series of investigated immediate actions to be applied after a cybercrime incident has occurred, for mediating consequences. As with the previous section the focus here is also type A offences. Despite the requisite reporting to national agency holding the relevant jurisdiction, further measures are introduced:

- Manually shut down the infected system, lock compromised accounts, and immediately protect personal, sensitive and identity information.
- Deployment of automated intrusion response system (AIRS), for appropriate response options to be automatically selected [17].
- Customer intrusion notification with concurrent blocking of traffic from specific address by ISPs, in cases of confirmed botnet detection.
- Skipping of root cause analysis of a confirmed type A incident, to prevent costs, interruption of businesses, etc.
- Immediate data backup and account information update.

The preventive and response measures and actions can be manually assigned to the introduced stakeholders, initiating the countering procedure. In Figure 3, measures and actions are proposed to stakeholders for a specific incident (hacking a personal computer), bearing in mind that the lists are indicative. The prior stage indicates preventive measures both general and customized for the reduction of incident frequency. The middle stage provides an accurate description of the identified offence that derived from the schema-based description of type A offences. Lastly, the post stage provides tackling actions in cases of pc hacking, such as blocking of compromised accounts and all incoming network traffic.

V. Discussion and Conclusions

The framework presented in this paper aims to a holistic approach in which particular framework views, deal with each separate aspect of an incident in an extensive and progressive way. In view I, the identification of cybercrime features generated a textual schema-based incident description that leads to improved understanding and management of incident occurrences. In view II, offences are categorized in an extensive two-level offence classification system that encompasses the most common forms of computer-related offences while its sustainability and usefulness is proved through comparison to existing taxonomies. In view III, by studying several recommendation surveys and guidelines, the authors identified typical and customized measures for preventing and tackling cybercrime, along with their respective stakeholders. The outcome of this view is a mechanism that can manually interconnect measures with the accountable ones, for all cybercrime incidents divided by type. The combination of separate views results in the proposed framework that utilizes a holistic approach towards cybercrime incidents. The framework, leads to: (a) better perception of a specific incident, (b) sustainable categorization of similar occurrences, and (c) efficient prevention and response regarding each type of offence, through assigning measures to stakeholders. The authors advanced previously published work through integrating the theoretical backbone of cybercrime with preventive and response measures, forming a potentially applicable framework. The authors are currently working on extending the proposed framework to an expert system aiming to automated incident management and detection/identification of cybercrime incidents through standard operating procedures and protocols.

References

[1] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.

[2] EUROPOL-European Cybercrime Centre (EC3), “Common Taxonomy for the National Network of CSIRTs (includes legal framework),” Jul. 2016.

[3] G. Tsakalidis and K. Vergidis, “A Systematic Approach Toward Description and Classification of Cybercrime Incidents,” *IEEE Trans. Syst. Man Cybern. Syst.*, vol. PP, no. 99, pp. 1–20, 2017.

[4] A. García Zaballos and F. González Herranz, “From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation,” Inter-American Development Bank, 2013.

[5] 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].

[6] M. Gercke, “Understanding cybercrime: Phenomena, challenges and legal response,” ITU, Sep. 2012.

[7] Council of Europe, “Convention on Cybercrime,” Budapest, 2001.

[8] 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].

[9] E. Mackenzie and K. Goldman, “Computer Abuse, Information Technologies and Judicial Affairs,” in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future*, New York, NY, USA, 2000, pp. 170–176.

[10] S. Ullah, M. Amir, M. Khan, H. Asmat, and K. Habib, “Pakistan and cyber crimes: Problems and preventions,” in *Anti-Cybercrime (ICACC), 2015 First International Conference on*, 2015, pp. 1–6.

[11] S. Verma and A. Singh, “Data theft prevention amp; endpoint protection from unauthorized USB devices #x2014; Implementation,” in *2012 Fourth International Conference on Advanced Computing (ICoAC)*, 2012, pp. 1–4.

[12] A. Almadhoob and R. Valverde, “Cybercrime Prevention in The Kingdom of Bahrain via IT Security Audit Plans,” *J. Theor. Appl. Inf. Technol.*, vol. 65, no. 1, pp. 274–292, 2014.

[13] W. Chung, H. Chen, W. Chang, and S. Chou, “Fighting cybercrime: a review and the Taiwan experience,” *Decis. Support Syst.*, vol. 41, no. 3, pp. 669–682, 2006.

[14] S. Malby, R. Mace, A. Holterhof, C. Brown, S. Kascherus, and E. Ignatuschtschenko, “Comprehensive study on cybercrime,” *U. N. Off. Drugs Crime Tech Rep*, 2013.

[15] Y. H. Alkandary and E. F. M. Alhallaq, “Computer Security,” *Computer*, vol. 5, no. 1, 2016.

[16] R. Shay *et al.*, “Designing Password Policies for Strength and Usability,” *ACM Trans. Inf. Syst. Secur. TISSEC*, vol. 18, no. 4, p. 13, 2016.

[17] Z. Wu, D. Xiao, H. Xu, X. Peng, and X. Zhuang, “Automated intrusion response decision based on the analytic hierarchy process,” in *Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on*, 2008, pp. 574–577.