Cybercrime Classification: A Victimology-Based Approach

Sayonnha Mandal  
University of Nebraska Omaha, USA  
smandal@unomaha.edu

Abstract: The need for understanding cybercrime and the possibility of its occurrence is significant to mitigate its adverse effects on society. A comprehensive universally agreed-upon classification scheme for cybercrime is hugely lacking in terms of utilizing a complete perspective of the entities involved in the same. A new perspective in cybercrime classification is moving beyond the machines and focusing on the humans, especially the victims. Cyber victimization extends from the single user to a mass or system perspective, thereby representing governments, organizations, and society to be categorized as victims. This paper proposes a novel ontological classification of cyber victimology that can help illustrate the complete cybercrime incident from the perspective of the victim. We utilize a multidimensional typology to represent the dimensions and classifications of the cybercrime victim. We then analyse the semantic relationships between the ontological objects to develop a comprehensive victimology representation. The understanding of the type and role of the victim provides new insight into the analysis of the cyber incident. Moreover, the resultant representation can serve as an extension to current cybercrime ontological frameworks and help in providing a new point of defence in cybercrime incidents. Finally, such a victimology-based classification can subsequently result in a dynamic ontology which can be queried to obtain relevant insights into the nature and occurrence of cybercrimes.

Keywords: Cybercrime, Victimology, Ontological framework, OWL

1. Introduction

In recent years, there has been an increase in cybercrime and consequently individuals, organizations and governments have all been negatively impacted. Cybercrime at present is endemic to society at large. Be it in the disruption of business and governments, impacting the lives of people and adversely affecting the economy, cybercrime is an ever-increasing phenomenon today. Moreover, the fact that these can be categorized as global crimes, due to the nature of transcending global boundaries in its impact as well as in its source, makes this a prominent aspect of current cybersecurity research. However, a single or standardized definition of the term “cybercrime” is largely lacking in computer science terminology. Donalds et. al. (2014) define the term as something “generally used to cover/describe a wide variety of illegal crimes or what is considered illicit conduct by individuals/groups against computers, computer-related and other devices, information technology networks, or traditional crimes, as well as actions targeting individuals, supported by the use of the Internet and/or technology.” Prominent cyber-attacks such as WannaCry ransomware have global impact, encrypting the theses and graduation projects of students in Chinese universities as well as leading to massive disruptions in medical procedures in Britain. The popular ransomware attack also affected Russia’s Health Ministry, Russian Railways and Russian and Spanish telecom companies Megafon and Telefonica respectively. French car company Renault and Brazil’s SSN office and FedEx were also some of the bigger organizations adversely affected by WannaCry (Donalds et. al, 2019).

Previous research has focused on the role of the device involved, nature of the attack and the viewpoint of the attacker or the defenders. To categorize and analyse these varied threats and attacks, various legal frameworks have been proposed. These include the Computer Security Incident Response Teams (CSIRTs) that target malicious cyber activities involving the use of information and communication technologies (ICTs). The role of law enforcement and their approach to cybercrime analysis has also been modified to implement knowledge centric policing. It has been identified that at least 30 categories of crime knowledge units are in use for police practice. These are demarcated into administrative, policing, legal, procedural, and analytical. A popular knowledge-based police approach is the Problem Oriented Policing or POP, a term coined by Herman Goldstein, which involves the use of four different types of knowledge to analyse crimes. Intelligence-led policing or I-LP, a more recent improvement on the POP method, approaches crime analyses based on “new” knowledge, which includes digital intelligence, data and information processing monitoring and demographic analysis to map crime patterns and methods. Several other similar Knowledge based systems or KBSs have been implemented in recent years in this field. These include the Integrated Ballistics Identification System (IBIS), Automated Palm and Fingerprint Identification System (AFIS), COPLINK Connect and POLNET (Donalds et. al, 2019). All the above-mentioned frameworks are, however, primarily focused on regular crimes, with very limited coverage of cybercrime in its entirety. With the advent of the Internet, connectivity, and ease of use of personal electronic devices, criminals are now committing traditional and new crimes using technology. According to Wall and April (2005), the Internet has enabled the rise of three aspects of criminal opportunity: traditional crimes such as
fraud, money laundering, pyramid schemes, stalking and sexually motivated crimes using technology, new
criminal activities such as Hacktivism, identity theft, 419 scams as well as opportunities for new types of digital
crimes such as e-auction scams, spam, DoS and DDoS attacks, hate speech and intellectual property infringement
and piracy. Hence the new push for KBS is to develop comprehensive frameworks that include the occurrence
and trends of cybercrime. The most popular form of cybercrime representation to date has been using
ontological models for cybercrime classification. The Crime emergency Event Model (CE2M) ontology was
developed to implement semantic level integration of all crime emergency service resources. A four-dimensional
approach was adopted by Hansman and Hunt (2005) to represent a computer and network attack classification
taxonomy. Kjaerland (2005) used factors such as source sector, impact, target, and method of operation as a
basis for classifying cybercrimes. In relatively recent years, the cybercrime taxonomies have been targeted at
categorizing their specific properties rather than the actual cybercrimes themselves. elements such as victim,
attacker, objective, tool and tactic, impact, result, relationship, target, and offense are typically used to classify
cybercrimes in an ontological domain. Although current cybercrime classification taxonomies assert a
comprehensive categorization of cybercrime characteristics, one aspect of these crimes have been heavily
neglected.

We believe that to provide a complete, holistic and a user centric perspective for current cybercrime trend, the
inclusion of a complete victimology profile of the user of the digital world is of utmost importance.
Understanding the victimology behind such incidents is effective in developing a complete picture of the
cybercrime event. Hence, a comprehensive analysis of cybercrime victimology is required to completely
understand cybercrimes from the perspective of the user as active vulnerability points. To assess a complete
picture of cybercrimes as crimes mediated by computer networks rather than crimes against machines, it is
necessary to analyse these crimes from different viewpoints. The focus of crime perspective has always typically
been from the point of view of the offender – the malicious actor or cybercriminal. However, a new approach in
the current millennium cybercrime definitions is moving beyond the machines, the attacker, and focusing on the
target humans, especially the victims. A new victimization typology of cybercrime has been proposed by
Jaishankar (2012, 2013) that identifies four targets of cyber victimization – Cyber victimization of Governments,
Cyber Victimization of Corporations, Cyber Victimization of Individuals or Interpersonal Cyber Victimization and
Victimless Crimes. Riding on this new approach and adopting the current cybercrime characteristic based
ontological representation, this paper proposes a novel outlook to cybercrime victimology-based ontology that
enhances present cybercrime taxonomies to provide an in-depth look through the perspective of the victim.

The rest of the paper is organized as follows: Section 2 provides a brief glimpse into various knowledge-based
taxonomies of cybercrimes and the popular ontological representations of cybercrime characteristics. In Section
3, the paper delves into the OWL ontological representation which inspires our work along with a discussion of
the victim typology classification. Section 4 describes how our model extends the previous representation to
include a comprehensive victimology perspective and demonstrates the resultant ontological model for
cybercrime victimology. Section 5 delves into an example application of our Victimology categories in real-world
cybercrime scenarios and discusses the limitations and improvements needed. We conclude our findings in
Section 6 with a discussion of our proposed future work.

2. Related Research

Previous research has investigated several models of cybercrime classification. The Hansman and Hunt (2005)
classification taxonomy included four dimensions and a specific vulnerability dimension and attack target
categorization. Although the elements proposed in this model are effective in classifying traditional cybercrimes,
it fails to include blended attacks. Choo (2011) defines blended attacks as a technique which utilizes both
semantic (exploiting human vulnerabilities) and syntactic (exploiting technical vulnerabilities) attack methods
against the victim. Inclusion of this category of blended attacks contribute to a more comprehensive cybercrime
ontology.

The four facetted cybercrime classification scheme was also utilized by Kjaerland (2005) to analyse attacks
against government and commercial sectors. It was successful in identifying new characteristics for cybercrime
classification, although it was limited in the inclusion of very few characteristics of cybercrime. Thus, this
taxonomy by itself fails to provide the comprehensive outlook we are striving for.

Simmons et. al. (2009) moved away from the four-dimensional approach to a five characteristic based approach
of cybercrime taxonomy. Coined AVOIDIT, this taxonomy uses Attack Vector, Operational Impact, Defence,
Information Impact, and Target as the five dimensions. A noticeable improvement on previous methods was the
inclusion of blended cyber-attacks as well as the analysis of the relationships between targets, hosts, access
paths and impacts. Although this taxonomy is a significant improvement over its predecessors, it still lacks a complete approach towards cybercrime, as it does not consider the attack classification, motive or objective of the attacker nor identifies the target victim of these attacks. Both these categories are important factors to be considered in providing a complete picture of cybercrime patterns.

In the domain of ontological framework development of cyber-attacks, van Herdeen, Irwin, Burke, ad Leenen (2012) proposed a taxonomy to represent network attacks. The resultant ontological framework utilized classes of attack scenario, actor, actor location, aggressor attack goal, motivation, scope size, scope, target, vulnerability, asset, sabotage, effect, phase, attack mechanism and automation level. The framework based on computer network attacks proved to be beneficial in identifying additional cybercrime characteristics such as the vulnerability and aggressor classes. However, the ontology suffers from the limitation that it does not encompass all types of cybercrimes. It fails to include blended attacks as well as victim specific targeted attacks, necessary for the comprehensive picture.

The categories and subjects’ approach were adopted by Applegate and Stavrou (2013) to describe a cyber conflict taxonomy. Subjects were identified as entities or events which represent real world cyber conflict events and its associated participants. Categories included two subcategories of actions and. Actors, which were further subdivided into further subcategories. This taxonomy served as an extension on the Simmons et al. version and was successful in refining more specific categories for cybercrime classification, along with the relationships among the elements. However, this taxonomy still suffers from its shortcomings in terms of the thoroughness of insights into a cybercrime incident. It fails to include attacker objective, the specific attack or offense and the resultant victim or complainant impacted, all of which are significant in building the complete cybercrime outlook.

The victim, attacker, objective, tool & tactic, impact, result, relationship, target, and offense characteristics approach was further adopted by Donalds and Osei-Bryson (2014) in their taxonomy focused on cybercrime properties rather than the nature of the crime. This approach enables identifying links between taxonomic characteristics and successfully integrates and extends previous classification schemes. Other relevant characteristics of cybercrime, namely attack event vulnerability and impact types were not considered as part of this taxonomy and hence were limited in these aspects.

An integrated view of cybercrimes was proposed by Barn and Barn (2016) and implemented in Protégé OWL (Web Ontology Language), which included a comprehensive classification of cybercrime characteristics. A variation from previous taxonomies was the inclusion of the “viewpoint of external observers”, which was significantly different from a law enforcement and policing based on CSIRT analyses. Moreover, the ontology combined traditional and cybercrime characteristics, which many researchers felt were easily captured using a technology subclass and not necessarily needed as a separate taxonomy element. Finally other relevant cybercrime concepts such as vulnerability, operational and informational impacts were not incorporated.

In terms of the role and impact of the user or human in cybercrimes, the research has been somewhat limited. Islam et. al. (2019) believes that the context of users and their relationships with the devices are mainly focused on the awareness and incentivization content. It fails to capture the ever-evolving user preferences and innovative attackers in a constantly changing cybersecurity and cybercrime landscape. The authors thus proposed a holistic socio-technical framework combining relevant concepts such as opportunity management, behavioural and business models. This framework aims to reduce human enabled risks in the cybercrime scenario by considering human roles of offenders, victims, preventers, and promoters. Although the framework considers the different user roles in cybercrimes, the focus is still on the attacker perspective and opportunity to reduce human related vulnerabilities of a system.

Philips et. al. (2022) in their research highlighted the importance of a comprehensive and standardized terminology and categorization of cybercrime elements. The push is towards building a comprehensive framework to conceptualize cybercrime after evaluating the existing definitions, typologies, and taxonomies prevalent in various law enforcement jurisdictions. However, the authors recognize that the resultant classification approaches come with their own weaknesses, specifically the failure to capture a holistic picture of the cybercrime. The authors believed that using a human perspective such as the motivations and intentions of the attacker may yield additional knowledge points in the framework representation.

The need for analysis of the human component of cybercrimes has led to increased attention to the cybercriminology division. Subramaniam et. al. (2022) observed several cybercrime frameworks and the lack thereof in different countries such as Malaysia and Nigeria and identified the need for a cyber victim intervention.
framework along with a cyber security framework. Recognition of cyber victims and victim studies were deemed to be significant aspects in the goal towards holistically protecting our cyberspace. Thus, our paper focuses on the importance of understanding cybervictimology and proposes a comprehensive ontological framework which includes the role and impact of cyber victims.

With the above discussion, it is evident that prior attempts at cybercrime classification have largely focussed on the different concepts of classification. These works have also used varying terminologies interchangeably, leading to a unified and standard approach for such taxonomic frameworks. Moreover, these non-adaptable frameworks are unable to account for ever changing dynamic and information for cybercrime incidents. This research also fails to demonstrate the complex relationships and interactions between framework elements as well as lacking the ability of the analysis of cybercrimes from varied perspectives.

Our proposed research aims to address all these shortcomings in our modified victimology-based taxonomy approach.

3. Background

This section explores the relevant background for the proposed research. We delve into the origin of the term Cybervictimology and its associated connotations. Further, we observe a typology for victims as published in previous research. This typology includes victim dimensions and their categorizations. Although the typology has been proposed for analysing victim profiles for traditional crimes, we draw a parallel of these classifications as applicable in our proposed framework of cybercrime specific victimization.

3.1 Cybervictimology

The terms cybercriminology and cybervictimology were first coined by K. Jaishankar in 2007 and 2015 respectively. Cybercriminology is defined to be a sub area of criminology, especially crimes involving the internet. The resultant victims of these crimes are considered cyber victims, and hence their study is known as cybervictimology. Cybercrimes are known by various terms such as digital crime, internet crime, virtual crime, e-crime or netcrime, they all represent the use of internet and communication networks to commit these crimes. However, compared to traditional crimes, victimization in cybercrimes is especially significant and distinct since, the cyber criminals do not necessarily need to be physically present or even close to the victims. An attacker can victimize any person anywhere in the world, just by using his devices and the internet. Also, the issue of timeline of the crime gets blurred as cybercrimes can automated and hence can occur over a given time range. Moreover, one crime can result in victimization of multiple people at a time with the same effort. Thus, the concept of victimization in the cybercrime context becomes important due to the nature of automation and the ability of offenders to impact rapidly and precisely many individuals at a time.

The Convention on Cyber Crime in the Council for Europe (2011) was one of the first entities who passed a legislation to consider cybercrime definitions from the victims (humans’ perspective rather than concentrating solely on the machines). The Convention identified offenses against children, attacks targeting human emotions, and the ban on improper words in cyberspace, instigating threats towards national security, racial hatred, and terrorism. Moreover, the perspective in identifying cybercrimes was shifted from only hacking or e-commerce attacks to include emotional attacks on users, and to evaluate attacks from the victim’s perspective. Wall (2008) first included the component of “harm” and “online insecurity and risk” in cybercrime definitions. This enabled the evaluation of impact of crimes like stalking, harassing, and bullying against human emotions. Cyber victimization, whenever recognized has also have had only a singular focus from the individual’s perspective and not from a mass or system perspective including governments, corporations, and society. Hence, considering these aspects is crucial for a complete definition of cyber victimization. Finally, the response of the victim and its effects in the overall cyberspace, which enables investigation of causes of re-victimization.

Haider and Jaishankar (2012) have since considered cybercrime from the victimization perspective and defined the terminology as follows:

“Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).”

The above definition encompasses all the following cybercrimes and associated abetment, towards individuals:
Hacking, Morphing, Spoofing, Computer source tampering, Obscene publication, Trojan attacks, Phishing, Cyber stalking, Cyber pornography, Cyber defamation, Cyber bullying, E-mail harassment, Cyber blackmailing, Cyber threats, Cyber murder, Cyber terrorism

Recognizing the wide array of cybercrime victimization aspects, our work seeks to demonstrate an easy-to-use model to explore the relevant elements in a typical cybercrime scenario and the association between the elements as viewed from the victim perspective.

3.2 Victim Typology

Landau and Freeman-Longo (1990) published research outlining a comprehensive classification of victim dimensions along with their different categorizations. We now take an in-depth look at the typology of a victim typically in the context of traditional crimes (Figures 1a and 1b). Our proposed research analyses elements from these typologies and implements the applicable ones in the final ontological model.

<table>
<thead>
<tr>
<th>Dimensions of Victimization</th>
<th>Individual</th>
<th>Group</th>
<th>Community</th>
<th>State</th>
<th>Corporate</th>
<th>Technological Environment</th>
<th>Interface Environment</th>
<th>Natural Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Legal Framework</td>
<td>Criminal Law</td>
<td>Civil Law</td>
<td>Transnational</td>
<td>International Law</td>
<td>No Legal Framework</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C. Irresponsibility of Perpetrator</td>
<td>Intentional</td>
<td>Recklessness</td>
<td>Negligence</td>
<td>Accident</td>
<td>Not Applicable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Identification of the Victim</td>
<td>Individual</td>
<td>Social Group</td>
<td>Corporate</td>
<td>Nation(s)</td>
<td>Mankind in General</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E. Victim Vulnerability</td>
<td>Age</td>
<td>Sex</td>
<td>Biophysical Characteristics</td>
<td>Psychological Characteristics</td>
<td>Social Characteristics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Victim's Perception of Victimization</td>
<td>Accurate self-perception of victim status</td>
<td>Inaccurate self-perception of victim status</td>
<td>Non-perception of victim status</td>
<td>Ignorance of the victimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1a: Dimensions and categorizations in a Victimology framework (Landau and Freeman-Longo, 1990)

<table>
<thead>
<tr>
<th>Accurate perception of victim status</th>
<th>Inaccurate perception of victim status</th>
<th>Non-perception of victim status</th>
<th>Ignorance of the victimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>G. Other's Perception of Victimization</td>
<td>Physical Harm</td>
<td>Sexual Abuse</td>
<td>Economic Damage</td>
</tr>
<tr>
<td>H. Type of Victimization</td>
<td>None</td>
<td>Mild</td>
<td>Moderate</td>
</tr>
<tr>
<td>I. Severity of Victimization/ Harm</td>
<td>Family</td>
<td>Acquaintance</td>
<td>Professional</td>
</tr>
<tr>
<td>J. Victim-Offender Relationship</td>
<td>None</td>
<td>Minimal</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Figure 1b: Dimensions and categorizations in a Victimology framework (Landau and Freeman-Longo, 1990) (continued)

3.3 Knowledge-Based Cybercrime Ontology

Donalds and Osei-Bryson (2012) presented a comprehensive cybercrime ontology based on the different elements present in a typical cybercrime scenario. The model identified the primary components for classification of cybercrime incidents the relevant relationships between them. The model was proposed to be extensible so that additional cybercrime characteristics and associated relationships can be added later as needed basis. Table 1 demonstrates the components of this cybercrime ontological model as proposed by the authors. The first column outlines all the elements discussed in the said ontology. The second column provides the definitions provided by the authors for these elements. Columns three and four demonstrate which of the elements have been utilized in our new extended cybervictimology model. As observed, for the purposes of this paper, we focus only on the 'Victim' element from the original model and discuss the typological classifications adopted and implemented in our ontology.
4. Our Approach

In the subsequent sub-sections, we discuss the proposed approach of building an ontology based on the cybervictimology classifications adopted.

4.1 Victimology-Based Cybercrime Approach

As mentioned previously, we adopt the CCO (Cybercrime Ontological) model, and its associated elements as defined in the ontological framework. Figure 2 shows the complete ontological representation as discussed in Donalds and Osei-Bryson (2012). The 'Victim' component (boxed in red colour) is the only one we have expanded as part of our current research. Since the purpose of our approach is to gather a different victim-based perspective on cybercrimes and their impact, the comprehensive expansion of this ontological element is the prime point of focus.

![Figure 2: Cybercrime Ontological Model (Donalds and Osei-Bryson, 2012)](image)

4.2 Cybercrime Victimology Ontological Model

To understand and implement effective policing for cybercrimes, there is a need for knowledge-based systems and applications. However, such methods specifically in cybercrime is largely lacking. Even with a few such frameworks in use, a comprehensive coverage of all elements of cybercrime and evaluation of different perspectives in the same are unexplored. In this research, we adopt an existing cybercrime knowledge-based
taxonomy and further enhance it by adding elements of cyber victimology. This enables the introduction of a victim-based perspective in cybercrime. We develop an ontological model of our modified victimology-based framework. An ontology is an efficient mechanism to capture knowledge in a particular domain and helps in conceptualizations of the domain elements into a human-understandable, but also a machine-readable format using objects, relationships, attributes, and axioms.

Our proposed cybercrime victimology framework considers all the above-mentioned victimization categorizations in its original format. However, the only place it differs from the original model is the categorization of Victims. We utilize the typology of victims outlined in Section 3.2 and expand the Victim attribute in the ontological model with its own categorizations and definitions as required. Although Section 3.2 has 11 categorizations (A-K) in the Victim typology, for our purposes of cybercrime victimization representation, we adopt a select set of these categories. We did not include the dimensions of Intentionality of the perpetrator, Victim’s perception of Victimization, and Others perception of Victimization, as these dimensions are more applicable to traditional crimes and victims rather than cybercrime. We assume that the cybercrime perpetrator has the intention of carrying out his actions and makes conscious choices to exploit vulnerabilities. We also remove the possibility of ambiguity in victim perception and for the purposes of our model assume a guaranteed impact of cybercrime events on the victims involved directly and indirectly. We represent our ontological model in Protégé OWL capturing the victimology aspects of cybercrimes as the expansion. The resultant ontological model for cybercrime victimology is provided in Figure 5. This model can be added on to the overall knowledge-based system model for cybercrimes discussed previously.

The 8 Cyber victimology typology dimensions and their associated categories, as adopted in the proposed model are as follows.

1. **Source of Victimization** (Individual, Group, Community, State, Corporate, Technological Environment, Interface Environment, Natural Environment)
2. **Legal Framework** (Criminal Law, Civil Law, Translational, International Law, No Legal Framework)
3. **Identification of the Victim** (Individual, Social Group, Corporate, Nation(s), Mankind in general)
4. **Victim Vulnerability** (Age, Sex, Biophysical characteristics, psychological characteristics, social characteristics)
5. **Type of Victimization** (Physical Harm/Damage, Sexual Abuse, Economic Damage, Psychological Damage, Damage to Reputation, Infringement of Civil/Human Rights)
6. **Severity of Victimization/Harm** (None, Mild, Moderate, Severe, Extreme, Maximal)
7. **Victim-Offender Relationship** (Family, Acquaintance, Professional, Stranger, Impersonal, Not Applicable)
8. **Victim’s Contribution to the Event** (None, Minimal, Moderate, High, Maximal)

Figure 3 shows the victimology typology dimensions that were adopted from Donalds and Osei-Bryson, 2012. The dimensions are represented as object classes and their relevant categories are represented as subclasses respectively.

![Figure 3: Victimology dimensions and categorizations as ontological class objects](image-url)
These object properties represent the following relationships between the victimology typology dimensions and their categorizations. The final ontological representation of the Cybercrime Victimology representation is illustrated in Figure 7 (provided at the end of the paper for better visibility).

Figure 4: Relationship between Victimology dimensions and respective categorizations as object properties

5. Classification of two Real World Cyber Attacks

In this section, we outline two real-world cybercrime cases as documented in the Sherloc UNODC database (to https://sherloc.unodc.org/). We highlight the relevant portions of the cases below for the sake of brevity. For the detailed case reports please go to https://sherloc.unodc.org/. We illustrate three more cases from the case law database in the appendix section of the paper. We focus on the victimization aspect only for these examples. The other attack aspects are covered in a similar manner to the Donalds et.al 2012 classification model. The following victimization dimensions and their corresponding categorizations were identified as follows:

5.1 Case DOMx001 (Identity Offence)

<table>
<thead>
<tr>
<th>Victimization Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of Victimization</td>
</tr>
<tr>
<td>Legal Framework</td>
</tr>
<tr>
<td>Identification of the Victim</td>
</tr>
<tr>
<td>Victim Vulnerability</td>
</tr>
<tr>
<td>Type of Victimization</td>
</tr>
<tr>
<td>Severity of Victimization/Harm</td>
</tr>
<tr>
<td>Victim-Offender Relationship</td>
</tr>
<tr>
<td>Victim’s Contribution to the Event</td>
</tr>
</tbody>
</table>

Figure 5: Case DOMx001 summary (https://sherloc.unodc.org/) and categorization
## 5.2 Case USAx209 (Forgery)

<table>
<thead>
<tr>
<th>Source of Victimization</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Framework</td>
<td>Civil Law, International Law</td>
</tr>
<tr>
<td>Identification of the Victim</td>
<td>Social Group, Nation</td>
</tr>
<tr>
<td>Victim Vulnerability</td>
<td>Sex, Psychological characteristics, Social characteristics</td>
</tr>
<tr>
<td>Type of Victimization</td>
<td>Psychological Damage, Infringement of Civil/Human Rights</td>
</tr>
<tr>
<td>Severity of Victimization/Harm</td>
<td>Maximal</td>
</tr>
<tr>
<td>Victim-Offender Relationship</td>
<td>Family</td>
</tr>
<tr>
<td>Victim’s Contribution to the Event</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

**Figure 6:** Case USAx209 summary ([https://sherloc.unodc.org/](https://sherloc.unodc.org/)) and categorization

### 5.3 Observations and Inferences

From an initial analysis of the above-mentioned real-world cybercrime cases and similar others from the database, we can highlight the following observations:

- The identity and details of the victim(s) are often hidden in traditional crimes and this practice has been present in cybercrimes as well. Hence, sufficient information on Victim characteristics such as Age, Sex, Social, Economic background, etc., has been largely missing from the cybercrime database case descriptions. Hence this categorization has not yielded the necessary information and the subsequent pattern expected from cybercrimes. Access to more detailed case descriptions from the law enforcement and legal case files are needed to make an accurate observation in this case.

- As with traditional crimes, the categorizations of cybercrime types into identity thefts, fraud, forgery, etc. are not mutually exclusive. Each of the cybercrime cases have elements of different categorizations that blur the lines to make effective demarcations of crime types difficult. For example, the case of DOMx001 has potential for charges under fraud as well as Identity offenses. Hence, either an overlap criterion for documenting these cases in an ontology should be studied and expressed appropriately in a framework.

- The details of the geographical extents of the victims are also missing in most cybercrime cases in the open-source databases. Like victim identities, their geographical locations can be useful in deciding applicability of local and international laws, relationship of victim and perpetrators, Victimization severity and Victim involvement. Detailed knowledge of these victim dimensions will provide a more complete picture of the crime from the victims’ perspectives, that will in turn enable possible patterns between the victims’ location, ease of access for the crime, prior relationship to the perpetrator, attempted social engineering attacks if any as well as legal precedents of similar cases from other countries if needed.

- The Victim dimensions and their corresponding categorizations have been effectively defined by Landau and Freeman-Longo (1990). However, more refined, and targeted definitions of these categories need to be established to fit the varying nature of cybercrime. As we observe, cybercrime victimization can span countries, different socio-economic groups and fall under different legal jurisdictions. Cybercrimes may also be encountered as a means or part of a traditional crime scenario and need a different approach of legal applicability and indictment. Hence, refining the provided definitions of victimizations to suitably fit cybercrime is justifiably needed. For example, Case USAx209 victims can be identified as both social group (the defendant’s original family in Pakistan) as well as the nation state of USA. Hence the justification of applying one or the other as part of the ‘Identification of Victim’ dimension are required for the ontological representation.
6. Conclusion and Future Work

In this paper, we outlined a taxonomic framework of cybercrime elements from the perspective of the victim. Including the victimology viewpoint in cybercrime analysis has received significant importance in recent times and a complete understanding of victimology patterns and details provide a holistic picture of a cybercrime classification system. We represented our model in Protégé OWL which provides an easy to visualize and explorable structure for different cybercrime elements. We followed a classic victimology typology and selected specific categories from it as appropriate for a cybercrime environment. We implemented a preliminary analysis of our model with real-world cybercrime descriptions. As part of our future work, we will attempt to generate an ontological representation of the incidents in a case study format. And observe and analyse victimology patterns to better understand and perfect cybercrime classification from the victimology perspective. Further work in this area will focus on developing SWRL rules to enable querying specific cybercrime details from the ontological model relevant to the case studies represented.

References

Appendix 1

Figure 7: OWL ontological representation of victimology dimensions and categorizations
Case FRAX030 (Forgery)

**Source of Victimization**
- Group

**Legal Framework**
- Criminal Law

**Identification of the Victim**
- Social Group, Corporate

**Victim Vulnerability**
- Social Characteristics

**Type of Victimization**
- Economic Damage

**Severity of Victimization/Harm**
- Severe

**Victim-Offender Relationship**
- Impersonal

**Victim’s Contribution to the Event**
- Minimal

---

Case ARGX016 (Fraud)

**Source of Victimization**
- Group

**Legal Framework**
- Criminal Law

**Identification of the Victim**
- Individual

**Victim Vulnerability**
- Psychological characteristics

**Type of Victimization**
- Economic Damage

**Severity of Victimization/Harm**
- Maximal

**Victim-Offender Relationship**
- Stranger

**Victim’s Contribution to the Event**
- High

---

Case USA217 (Identity Offence)

**Source of Victimization**
- Group

**Legal Framework**
- Criminal Law

**Identification of the Victim**
- Corporate

**Victim Vulnerability**
- Inadequate data

**Type of Victimization**
- Economic Damage, Damage to Reputation

**Severity of Victimization/Harm**
- Severe

**Victim-Offender Relationship**
- Professional

**Victim’s Contribution to the Event**
- Maximal