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. (2014) al defines 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.

A Conceptual Framework for Victimology: The Dimensions and their Categories

Dimensions	1	2	3	4	5	6	7	8
A. *Source of Victimization*	Individual	Group	Community	State	Corporate	Technological Environment	Interface Environment	Natural Environment
B. *Legal Framework*	Criminal Law	Civil Law	Transnational, International Law	No Legal Framework				
C. *Intentionality of Perpetrator*	Intentional	Recklessness	Negligence	Accident	Not Applicable			
D. *Identification of the Victim*	Individual	Social Group	Corporate	Nation(s)	Mankind in General			
E. *Victim Vulnerability*	Age	Sex	Biophysical Charac-teristics	Psychological Charac-teristics	Social Charac-teristics			
F. *Victim's Perception of Victimization*	Accurate self-perception of victim status	Inaccurate self-perception of victim status	Non-perception of victim status	Ignorance of the victimization				

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

G. *Other's Perception of Victimization*	Accurate perception of victim status	Inaccurate perception of victim status	Non-perception of victim status	Ignorance of the victimization			
H. *Type of Victimization*	Physical Harm/ Damage	Sexual Abuse	Economic Damage	Psychological Damage	Damage to Reputation	Infringement of Civil/ Human Rights	
I. *Severity of Victimization/ Harm*	None	Mild	Moderate	Severe	Extreme	Maximal	
J. *Victim-Offender Relationship*	Family	Acquaintance	Professional	Stranger	Impersonal	Not Applicable	
K. *Victim's Contribution to the Event*	None	Minimal	Moderate	High	Maximal		

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 an 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.

Table 1: Cybercrime classification ontological concepts

Element Name (Old Model)	Definition (Old Model)	Use in New Model (No Change)	Use in New Model (Changed
Attack_Event	*"Actual real-world cybercrime or nefarious cyber action committed by an Attacker"*	✓	
Vulnerability	*"Actual real world cybercrime or nefarious cyber action committed by an Attacker"*	✓	
Tool_and_Technique	*"Tool and/or technique used by an Attacker to execute a cyber action"*	✓	
Objective	*"The main purpose, motive or end goal of an Attacker for committing a cyber event"*	✓	
Offence	*"An illicit cyber action or event"*	✓	
Location	*"Country and/or specific address of an individual/group Attacker, the Victim and/or Target that experiences the event"*	✓	
Complainant	*"One who reports a cyber event, making the authorities aware of the illicit activity"*	✓	
Victim	*"An entity that is affected in some way by a cyber event"*		✓
Target	*"An entity that a cyber event is specifically directed at"*	✓	
Impact	*"The direct effect caused by a cyber event on a Victim"*	✓	
Attacker	*"Criminals trying to exploit resources for personal, governmental and financial goals. "*	✓	

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.

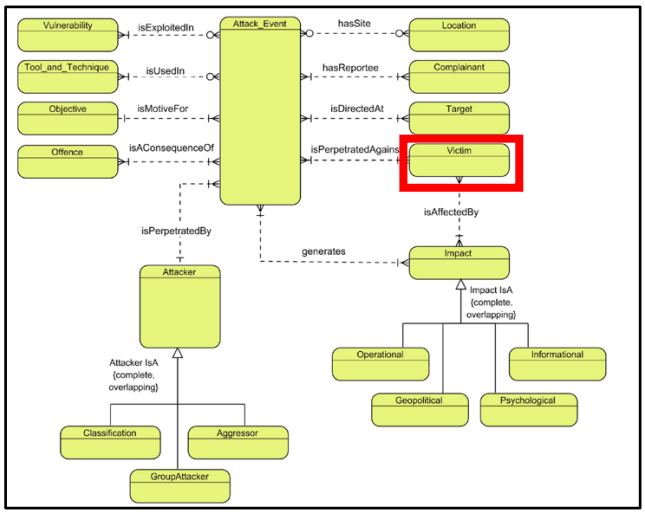

Figure 2: Cybercrime Ontological Model (Donalds and Osei-Bryson, 2012)

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 for4mat. 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.

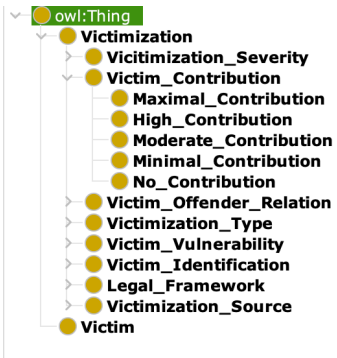

Figure 3: Victimology dimensions and categorizations as ontological class objects

Figure 4 demonstrates the ontological representation of the relationships between the object classes. We define 9 new object properties to represent the relationships between each of the victimology dimensions and their respective categories.

1. Victimization ------←--------isRelatedAs---------←------ Victim_Offender-Relation
2. Victimization ------←--------hasInvolvement---------←------ Victim_Contribution
3. Victimization ------←--------causesResults---------←------ Victimization_Type
4. Victimization ------←--------hasIntensity---------←------ Victimization_Severity
5. Victimization ------←--------isIdentifiedAs---------←------ Victim_Identification
6. Victimization ------←--------isGovernedBy---------←------ Legal_Framework
7. Victimization ------←--------isInitiatedBy---------←------ Victimization_Source
8. Victimization ------←--------isCausedBy---------←------ Victim_Vulnerability
9. Victimization ------←--------undergoes---------←------ Victim

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).

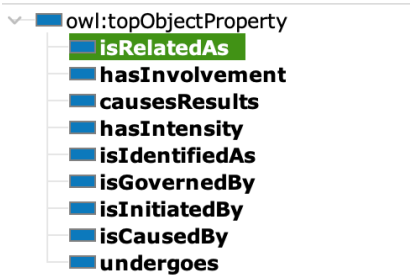

Figure 4: Relationship between Victimology dimensions and respective categorizations as object properties

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)

DOMx001 **Segundo Tribunal Colegiado De La Cámara Penal Del Juzgado De Primera Instancia Del Distrito Nacional, Sentencia penal núm. 249-04-2021-SSEN-00225**

Dominican Republic

Verdict Date: 2021-11-04
Sentence Date: 2021-11-04

In 2018, the two defendants, Eric Antonio Morel Garcia and Henry William Cruz, along with others (Rafael Leónidas Sepúlveday and Winifer Hernández) defrauded the victim by fraudulently obtaining access codes to her bank accounts, which allowed them to conduct multiple electronic transfers of fraudulent funds in the total amount of DOP 2,336,000.00. The victim was contacted by a person who self-identified as Doña Carmen, pretending to be the person who will manage her Cibao Savings and Loans Association accounts. "Doña Carmen" informed the victim that she should go to the bank branch and request a code card to activate Internet Banking. The victim was subsequently contacted multiple times by "Doña Carmen" requesting the card code access, under the pretext that the person was adjusting her bill. When the victim received credit card transactions she contacted "Doña Carmen" who told her it was a platform problem.

Victimization Analysis	
Source of Victimization	Group
Legal Framework	Criminal Law
Identification of the Victim	Individual
Victim Vulnerability	Inadequate data
Type of Victimization	Economic Damage
Severity of Victimization/Harm	Moderate
Victim-Offender Relationship	Stranger
Victim's Contribution to the Event	Moderate

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

5.2 Case USAx209 (Forgery)

USAx209 **United States of America v. Khan, No. 17-4301 (4th Cir. Apr. 4, 2018)**

United States of America

Verdict Date: 2020-04-04
Sentence Date: 2018-04-04

This case involves several offences, including conspiracy, smuggling cultural property into the U.S., obstruction of justice, and citizenship and naturalization fraud, committed by the defendant Ijaz Khan with the assistance of several co-conspirators. In 2002, the co-conspirator Vera Lautt travelled to Pakistan to meet Ijaz Khan, whom she had met online, and to sign marriage documents. Subsequently, they both submitted fraudulent documents to the U.S. Department of State (DOS) and U.S. Citizenship and Immigration Services (USCIS), facilitating the immigration and later naturalization of Ijaz Khan. The defendant Ijaz Khan was, however, still married to a Pakistani woman, with whom he had and continued to have children, at the time of and after signing the marriage documents. According to the indictment, Ijaz Khan used his citizenship to enable the immigration and later naturalization of his four oldest sons. He divorced Lautt before the children had arrived in the United States. He further filed or assisted with petitions on behalf of his brother, Ibar Khan, his Pakistani wife, his mother, and another two children.

Victimization Analysis	
Source of Victimization	Group
Legal Framework	Civil Law, International Law
Identification of the Victim	Social Group, Nation
Victim Vulnerability	Sex, Psychological characteristics, Social characteristics
Type of Victimization	Psychological Damage, Infringement of Civil/Human Rights
Severity of Victimization/Harm	Maximal
Victim-Offender Relationship	Family
Victim's Contribution to the Event	Moderate

Figure 6: Case USAx209 summary (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

Applegate, Scott D., and Angelos Stavrou. "Towards a cyber conflict taxonomy." *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. IEEE, 2013.

Barn, Ravinder, and Balbir Barn. "An ontological representation of a taxonomy for cybercrime." (2016).

Blythe, John M., and Lynne Coventry. "Costly but effective: Comparing the factors that influence employee anti-malware behaviours." Computers in Human Behavior 87 (2018): 87-97.

Choo, Kim-Kwang Raymond. "The cyber threat landscape: Challenges and future research directions." Computers & security 30.8 (2011): 719-731.

David, Wall, and Pattavina April. "The Internet as a conduit for criminal activity." Information technology and the criminal justice system. Sage, 2005. 77-98.

Wall*, David S. "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime." International Review of Law, Computers & Technology 22.1-2 (2008): 45-63.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. "A cybercrime taxonomy: case of the Jamaican jurisdiction." (2014).

Donalds, C. M., and K. M. Osei-Bryson. "The construction of A domain ontology for criminal investigation: The case of the Jamaican constabulary force." SIG ICT in Global Development, 5th Annual Pre-ICIS Workshop, Orlando, FL. 2012.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. "Toward a cybercrime classification ontology: A knowledge-based approach." Computers in Human Behavior 92 (2019): 403-418.

Guarino, Nicola, and Pierdaniele Giaretta. "Ontologies and knowledge bases." *Towards very large knowledge bases*(1995): 1-2.

Hansman, Simon, and Ray Hunt. "A taxonomy of network and computer attacks." *Computers & Security* 24.1 (2005): 31-43.

Van Heerden, Renier P., et al. "A computer network attack taxonomy and ontology." International Journal of Cyber Warfare and Terrorism (IJCWT) 2.3 (2012): 12-25.

Islam, Tasmina, et al. "A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems." *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications*. Singapore: Springer Singapore, 2019.

Jaishankar, K. "Cyber victimology: a new sub-discipline of the twenty-first century victimology." *An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen* (2020): 3-19.

Keyser, Mike. "The council of Europe convention on cybercrime." Computer Crime. Routledge, 2017. 131-170.

Kjaerland, Maria. "A taxonomy and comparison of computer security incidents from the commercial and government sectors." Computers & Security 25.7 (2006): 522-538.

Landau, Simha F., and Robert E. Freeman-Longo. "Classifying victims: A proposed multidimensional victimological typology." *International review of victimology* 1.3 (1990): 267-286.

Phillips, Kirsty, et al. "Conceptualizing cybercrime: Definitions, typologies and taxonomies." *Forensic sciences* 2.2 (2022): 379-398.

https://sherloc.unodc.org/

Simmons, Chris, et al. "AVOIDIT: A cyber-attack taxonomy." *University of Memphis, Technical Report CS-09-003* (2009).

Subramaniam, S., Ratha Krishnan, S. & Sathakathulla, S.A. 2022. Cyber Victim Intervention Framework: An Introduction. Selangor Women Conference 2022. Selangor Journal.

Tsakalidis, George, et al. "A cybercrime incident architecture with adaptive response policy." *Computers & Security* 83 (2019): 22-37.

Appendix 1

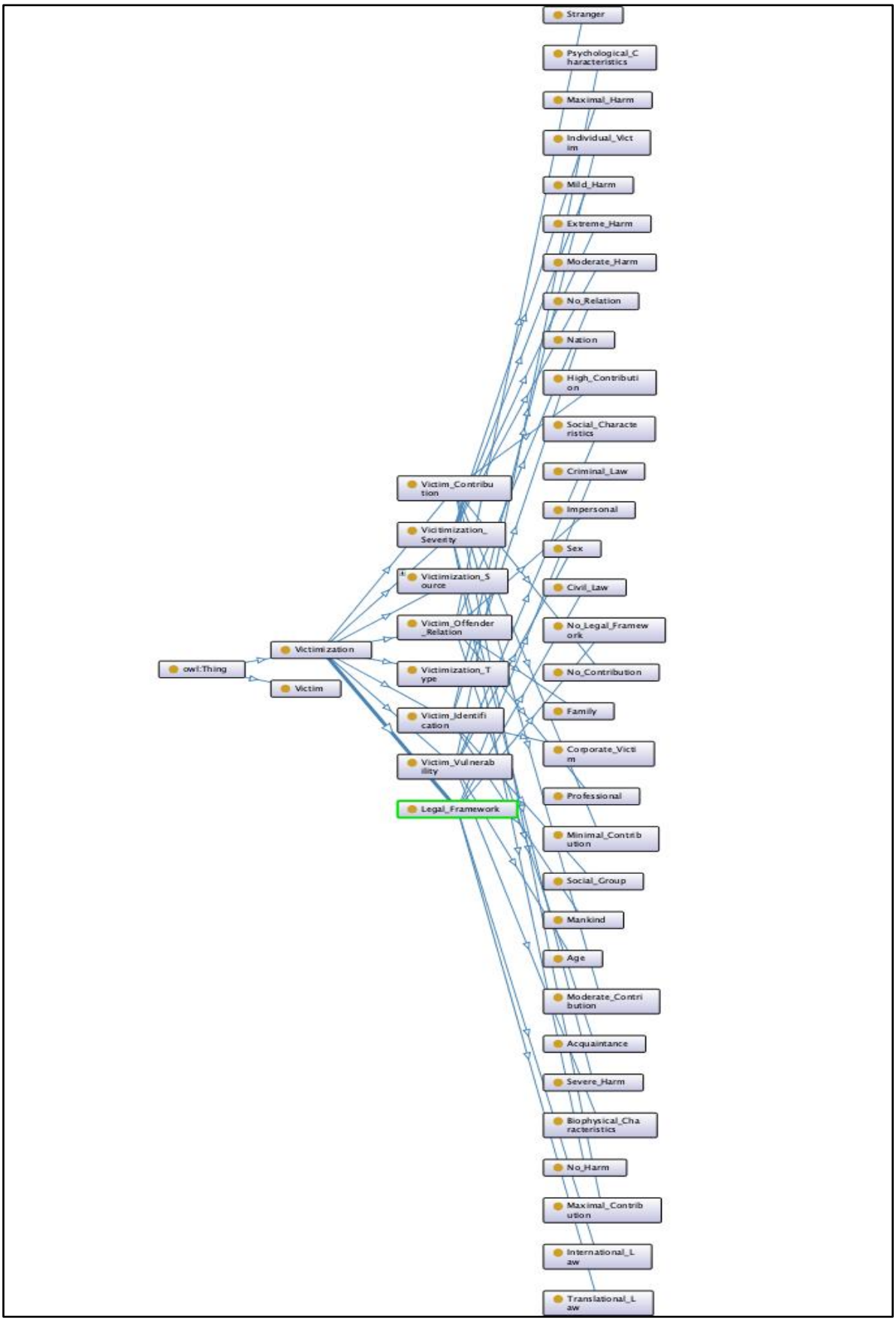

Figure 7: OWL ontological representation of victimology dimensions and categorizations

Case FRAx030 (Forgery)

FRAx030 **TGI Paris, 13e ch. corr., jugement du 20 novembre 2018**

France

Verdict Date: 2018-11-20
Sentence Date: 2018-11-20

From 2010 to 2014, the defendant Mr Z. conducted a criminal enterprise to fraudulently purchase goods on commercial websites. To this end, Mr Z. used stolen credit card data found on carding forums by himself, Mr P. (the technical advisor of the group) and Mr N. (a member of the group in charge of finding credit card data), as well as credit card data that Mr L. had stolen from his former employer. Mr P. and Mr Z. would then hack into customer accounts on commercial websites and modify their contact information so that the actual customer would not receive any notification of purchase and/or delivery. Mr Z. and N. would then buy goods on commercial websites and send them to parcel collection points. Mr Z and Mr X forged fake IDs and used mules to receive the packages at the collection points. Several people were used as mules: Messrs Y, M, O, Q, V, T, and R. The mules would receive the packages, keep some packages as payment and send the others to Mr Z. so that he could sell them on retailer websites. Several people involved in this criminal organization later started using the same techniques to buy goods on their own behalf.

Victimization Analysis	
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)

ARGx016 **Juzgado En Lo Correccional Nº 1 - San Isidro, Case No. SI-3862-2021**

Argentina

Verdict Date: 2022-03-22
Sentence Date: 2022-03-22

A criminal group, including the defendant XXX, committed fraud by masquerading as a Banco Galicia employee. The group sent an Instagram message to the victim informing her that if she wanted to receive advice from the financial institution, she should provide her cell phone and her area code. She subsequently received calls from two numbers from the Province of Córdoba via WhatsApp from someone pretending to be an employee of the Bank Galicia (this person was still unidentified at the time of this case). The person who called the victim tricked her into providing her banking details and her security token. The victim's information was then used to obtain a loan in the amount of ARS 189,448.00, which was later transferred together with the additional money contained in the victim's account, making it a total of ARS 229,000.00, to an account in the name of the defendant. The money was then transferred to another account of the defendant and an account of XXX. They in turn then transferred the money to others (YYY, ZZZ and OOO).

Victimization Analysis	
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 USAx217 (Identity Offence)

USAx217 **United States of America v. Wyatt, No. 4:17-cr-00522-RLW-SPM (E.D. Mo. Sept. 21, 2020)**

United States of America

Verdict Date: 2020-09-21
Sentence Date: 2020-09-21

This case involves a member of the cyber organized criminal group "The Dark Overlord" (TDO), an organization that was known for their ransom and extortion scams. Beginning in 2016, the defendant was involved in a conspiracy that encompassed hacking several organizations in health, entertainment, finance, commercial, real estate, and transportation, stealing personal information from the systems they hacked, including for instance medical records, and then seeking ransom from the targets. Companies would usually have to pay a ransom of between USED 75,000 and 350,000 in bitcoin. The defendant's role in the conspiracy was creating, validating, and maintaining communication, payment, and virtual private network accounts that were, inter alia, used to send threatening and extortionate messages to the victimized companies within the Eastern District of Missouri, where the defendant was ultimately tried.

Victimization Analysis	
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