An Ontological Approach to Classifying Cybercrimes in an ICT4D Context

Charlette Donalds[1(✉)] and Kweku-Muata Osei-Bryson[2]

[1] University of the West Indies, Mona Kingston, Jamaica
charlette.donalds02@uwimona.edu.jm
[2] Virginia Commonwealth University, Richmond, USA
KMOsei@VCU.edu

Abstract. While the phenomenon of cybercrime remains a challenge for governments worldwide, it is even more of a challenge for countries in an ICT4D context since they possess limited technical skills and resources to respond to, investigate and prosecute nefarious cyber activities. Despite the challenges, governments have responded by establishing legal frameworks and Computer Security Incident Response Teams. However, scholars argue that the cybercrime phenomenon is still not well understood; which is compounded by the lack of an accepted, uniform cybercrime classification scheme or ontology with which to classify cybercrimes. While few classification schemes have been published, same are limited in that they are not comprehensive; i.e., they are unable to account for the range of and ever changing types of cybercrimes and, the schemes are largely incompatible, focusing on different perspectives. This makes holistic and consistent classification improbable. To address these gaps we propose a formal cybercrime classification ontology, expressed in OWL Ontology Language. In designing our ontology we were guided by the steps of the design science research methodology. This paper contributes a formal ontology of a 'shared conceptualization' of cybercrimes by police practitioners and researchers. The ontology presented here is improved over prior works since it incorporates multiple perspectives and its design is better able to handle existing and future cybercrimes, a most salient feature given the dynamic nature of cybercrimes. We demonstrate the ontology by applying it to an actual cybercrime case. The designed ontology effectively classifies the cybercrime and has the potential to improve cybercrime classification in ICT4D and developed contexts.

Keywords: Cybercrime classification · Ontology · Developing country

1 Introduction

Cybercrime remains a fundamental concern for citizens, organizations and governments worldwide. With the increasing proliferation of integrated digital technology into objects and the World Wide Web being the universal medium for conducting business and for socialization, security issues such as unauthorized access to, interception of, interference with data, computer related fraud and forgery, et al., are now major challenges. Also, the financial consequences of cyber-related incidents are dire and is

S. Chatterjee et al. (Eds.): DESRIST 2018, LNCS 10844, pp. 253–267, 2018.
https://doi.org/10.1007/978-3-319-91800-6_17

worsening. According to the Ponemon Institute and Accenture [1], cybercrimes cost organizations, on average, US$11.7 million in 2017, representing a 23% increase over 2016.

An upsurge in cybercrime in some Commonwealth Caribbean countries has also been reported. According to the Commonwealth Cybercrime Initiative, some reported incidents in the region include the theft of US$150 million from the Bank of Nova Scotia in Jamaica in 2014; individuals claiming to be local ISIS supporters hacked government websites in 2015; and, in the same year, tax authorities in the region were infected by ransomware, which blocked users from accessing their systems and demanded money for users to regain access [2]. This trend in the Caribbean is even more troubling than for developed nations as more and more governments increase the use of Information and Communication Technologies (ICTs) to deliver services to its people without the commensurate technical and administrative capabilities to combat these emergent threats. Notwithstanding, the Caribbean counties have formally recognized that combatting cybercrimes and strengthening their cyber resilience are imperatives to economic and social development; democratic governance, and national and citizen security [3].

In response to cybercrimes, governments worldwide and in the Caribbean specifically, have in recent years developed legal frameworks and established Computer Security Incident Response Teams (CSIRTs also commonly referred to as CERTs or CIRTs) to better respond to, investigate, and prosecute nefarious cyber activities or crimes involving the use of ICTs [3]. However, scholars argue that the phenomenon of cybercrime is still not well understood. In fact, they posit that a better understanding of cybercrimes is necessary: (1) to develop appropriate legal and policy responses; (2) to develop better estimates of the economic costs of cybercrimes on society; and (3) for educating the public about the types of cybercrimes [4]. Researchers argue further that the problem is compounded by the lack of an accepted, uniform cybercrime classification scheme or ontology with which to classify cybercrimes. According to Ngo and Jaishankar [5], a universally agreed-upon classification scheme is necessary to advance our knowledge and the scholarship of cybercrime. Other scholars [6] posit that a consistent classification scheme is needed for cross jurisdictional cooperation, information sharing and for the successful prosecution of cybercriminals.

Despite the magnitude of the cybercrime phenomenon, there is a dearth of research focusing on a cybercrime classification scheme [see 4, 7–9] and even fewer yet on a cybercrime ontology [see 4]. Albeit, the published classification schemes are limited in that they are not comprehensive; i.e., they are unable to account for the range of and ever changing types of cybercrimes. Further, these classification schemes are incompatible, focusing on different perspectives and/or using varying terminologies interchangeably, even though they refer to the same thing. This makes consistent and repeatable cybercrime classification difficult. However, consistent and repeatable classification is salient to the area. Arguably, it can enable researchers and practitioners to predict the direction of future cybercrimes as well as formulate novel and timely solutions [5]. To achieve repeatable and consistent classifications, their needs to be a shared conceptualization of cybercrimes. This shared conceptualization provides a common, consistent language that can be used by all cybercrime stakeholders.

To address these research gaps, we develop a comprehensive cybercrime classification ontology, expressed in OWL ontology language. Furthermore, this work is part of a larger project that aims to develop a cybercrime reporting tool for a police organization in a Caribbean country. The objective is that the cybercrime tool will be able to collect, classify and provide trending information about cybercrimes. This ontology then, is an initial step towards such an effort; and aims to provide a 'shared conceptualization' of cybercrimes by police practitioners and researchers. A conceptualization has been described by Gruber [10] as an abstract, simplified view or model of a domain of interest.

An ontology is described as an "an explicit specification of a conceptualization" [10] which captures objects, concepts, entities and the relationships that hold among them. Some advantages presented in the literature [11] for adopting an ontology are: (1) Common vocabulary - it defines a common vocabulary for stakeholders who need to share information in a domain. (2) Sharing – facilitates the sharing of a common understanding of the structure of information among stakeholders in a domain or software agents; (3) Reuse – enables the reuse of domain knowledge; and (4) facilitates the analysis of domain knowledge.

The remainder of this paper is organized as follows: in Sect. 2 we present our research approach and works related to our study. Section 3 describes the research methodology and in Sect. 4 we present the conceptual model of our ontology, represented as an entity relationship diagram (ERD). In Sect. 5 we then present our ontology, expressed on Protégé OWL and demonstrate the efficacy of our ontology by using it to classify an actual cybercrime. We present concluding remarks and future research plans in Sect. 6.

2 Research Approach and Related Work

2.1 Research Approach

Our cybercrime classification ontology is based primarily on the taxonomy presented by Donalds and Osei-Bryson [7], hereafter referred to as the base taxonomy. That is we adopt/adapt the taxonomic characteristics proposed by [7]. Notably, in this study other related works augment our proposed ontology. We believe that the base taxonomy is a good starting point for several reasons: (1) during its development the authors incorporated properties of a sufficient and acceptable taxonomy in its design (such as 'useful', 'accepted', 'unambiguous', 'established terminologies', 'complete', et al.); (2) it incorporates several perspectives to more holistically classify cybercrimes (such as 'attacker', 'victim', 'offense', 'objective', 'tactic and tool', 'impact', et al.); (3) its uses the concept of characteristic structure, i.e., it classifies properties about that which is being classified and not the object itself, making it easily extendable.

The approach in grounding our work on a taxonomic structure is acceptable and is also described as an important step in the ontology development process. For instance, researchers [12] indicate that a "baseline taxonomy" forms the basis of the "seed ontology" (i.e., the initial ontology) in the ontology development process. Other researchers [13, p. 2] note that "an ontology subsumes a taxonomy" and Noy and

McGuinness [11, p. 3] indicate that building an ontology includes "arranging the classes in a taxonomic (subclass – superclass) hierarchy". Further, this approach has also been used in other works [see for example 4, 14].

2.2 Related Work

While there is a growing body of literature about cybercrimes, not much focus has been given to the use of ontologies for the classification of such crimes. However, some prior works have been done in the area of network and computer related attacks, which we think are pertinent and are therefore included in this review. Network and computer attacks are relevant to this area since they too are described as types of cybercrimes. For instance, in the Convention on Cybercrime [15] these types of cybercrimes are described as attacks against computer systems, networks and infrastructure.

Donalds and Osei-Bryson [7] proposed a taxonomy with nine characteristics, which arguably provides a more holistic classification scheme for cybercrimes. This taxonomy provides assistance in improving the classification of cybercrimes as well as consistency in language with regards to cybercrime events. Specifically, *Victim*, *Attacker*, *Objective*, *Tool & Tactic*, *Impact*, *Result*, *Relationship*, *Target* and *Offence* are the proposed taxonomic characteristics. While improved, the taxonomy is still limited. For instance, it does not address vulnerabilities via which the cybercrimes may occur nor identify the types of impacts that may affect a victim.

van Herdeen et al. [14] presented a computer network attack taxonomy and ontology with *Attack Scenario* as the core class to characterize and classify network attacks. Other taxonomy and ontology classes include, *Actor*, *Actor Location*, *Motivation*, *Target*, *Aggressor*, *Vulnerability*, *Phase*, *Attack Goal*, *Automation Level*, *Attack Mechanism*, *Effects*, *Sabotage*, *Scope and Scope Size.* Some classes also had sub-classes; for instance, the Actor class was divided into subclasses: *Group Actor*, *Hacker*, *Insider* and *Unknown Actor* and the Aggressor class: *State*, *Commercial Aggressor*, *Individual Aggressor*, *Self Instigator* and *Unknown Aggressor*. This network attack taxonomy and ontology is useful in that additional classes not previously identified for cybercrimes can now be incorporated in future works. For instance, in our ontology we incorporate *Vulnerability* and our *Attack_Event* is analogous *to Attack Scenario*. Notwithstanding, this ontology also has limitations. For instance, it is not able to classify cybercrimes against individuals and therefore lacks pertinent information that would be beneficial for knowledge bodies such as CSIRTs that classify cybercrimes on a day-to-day basis, and for the type of organization that our ontology is being developed for.

Using facet theory and multidimensional scaling (MDS) Kjaerland [16] analyzed cyber-intrusions reported to a CERT and identified a four faucet cyber incident taxonomy. The four facets are: *Source*, *Impact*, *Target* and *Method of Operation*. Using the four facets, Kjaerland analyzed government incidents vis-à-vis commercial. This taxonomy is useful in several ways: (1) it identifies new concepts that improve or knowledge and that which can also be incorporated in future works on cybercrime classification; and (2) it attempts to classify cybercrimes based on characteristics. However, the taxonomy is limited. Like most other cybercrime classification

taxonomies, it too focuses on only few areas via which to classify cybercrimes, thus it is lacking the details needed for thorough insight into and complete classification of cybercrimes.

Barn and Barn [4] presented a taxonomy for cybercrimes, which formed the basis of their proposed cybercrime classification ontology. The ontology presented the following classes: *Agent*, *Action*, *Contact*, *External Observer*, *Impact*, *Location*, *Motivation*, *Target*, *Technology Role* and *Viewpoint*. To evaluate their proposed ontology, the authors used two well-known cybercrime examples: the Nigerian 419 scam and the CryptoLocker malware. The authors present an informative ontology which uses several perspectives with which to classify cybercrimes. Additionally, it identifies additional concepts that improves our understanding about cybercrimes. Notwithstanding, this ontology is limited; it lacks the details needed for thorough insights into cybercrimes. For instance, it does not capture the various types of attackers (e.g., blackhat, script kiddies, et al.) nor does it distinguish between a target and the victim; both are not necessarily one and the same. Additionally, the authors present a high level view of *Viewpoint* without providing enough detail about *Action_View* and *CrimeView*, subclasses of *Viewpoint*.

Our ontology is improved over existing works in several areas: (1) it incorporates varying and multiple cybercrime perspectives and therefore should provide a more holistic and complete scheme with which to classify cybercrimes; (2) its' structure is flexible, i.e., our ontology classifies cybercrimes based on properties of the cybercrime and not the actual cybercrime itself. Therefore, it is arguably better able to handle existing and future cybercrimes, a most salient feature given the dynamic nature of cybercrimes; and (3) it is adaptable, i.e., it can be easily extended in terms of new concepts and new types of cybercrimes.

3 Methodology

In this research we adopt a design science (DS) approach in designing our cybercrime classification ontology (CCO). DS, as conceptualized by Simon [17], is a research paradigm that produces innovative artifacts to solve real-world problems. Additionally, DS involves a rigorous process to design artifacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences [18]. Artifacts can take several forms and may include constructs, models, methods and instantiations [18, 19]. In this research, the artifact is the cybercrime classification ontology expressed in the OWL Ontology Language (OWL).

We applied the design science research methodology (DSRM) proposed by Peffers et al. [19] in developing our artifact. We chose the DSRM since: (1) it builds upon the strengths of prior efforts that proposed guidelines for conducting DS research; and (2) we concur with others [20] that it provides a useful synthesized general model. In Table 1 we indicate the steps of the DSRM and discuss how it is applied to this research.

Table 1. DSRM steps and application.

DSRM Step	Research application
Problem identification and motivation	In Sects. 1 and 2 we have established the importance and relevance of our research problem
Define solution objectives	The objectives of the solution have been inferred from the problem definition, which seeks to explain how the artifact would address the stated problem(s). The objectives of the study addresses current research gaps by proposing a more comprehensive artifact with which to classify cybercrimes; and, is more adaptive in that new terms and concepts can be easily added
Design and development	In Sects. 4 and 5 we have presented the conceptual design as well as the cybercrime artifact, respectively
Demonstration	In Sect. 5 we have demonstrated the use of the artifact by classifying an actual cybercrime.
Evaluation	Evaluation of the effectiveness of the artifact and possible redesign will be conducted in our next step after the artifact is implemented in a developing country police organization and used by cybercrime investigators to classify cybercrimes
Communication	This paper represents an attempt to communicate the problem and its importance, the artifacts' design and its effectiveness to the research community

4 Conceptual Model

In this section we present the conceptual model of our cybercrime classification ontology. Figure 1 provides a general overview of the ontology with the main concepts and the relationships between them. Below, each concept in the conceptual model is discussed.

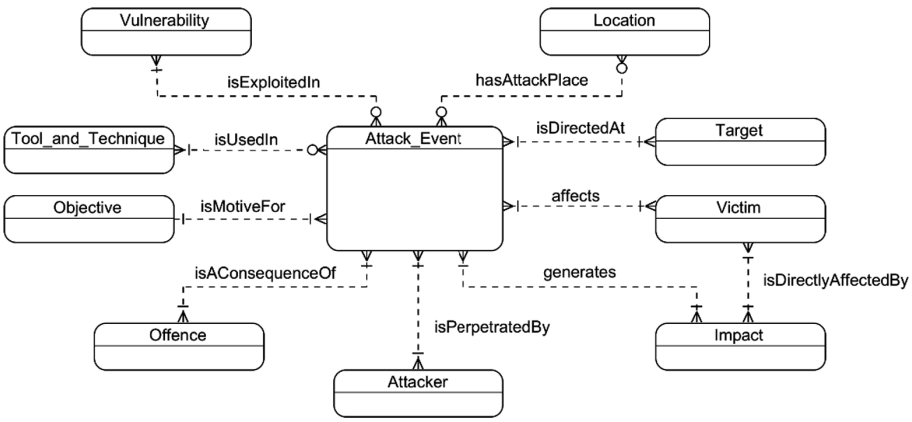

Fig. 1. Cybercrime classification conceptual model.

4.1 Attack_Event

The *Attack_Event* is central to our conceptual model and is used to capture the type of cybercrime/action that has been perpetrated by an *Attacker*. Examples of *Attack_Events* are: virtual sit-ins, hacking of email servers, denial of service (DoS), website defacement, site redirects, et al. Properties about the *Attack_Event* such as the start and end dates of the attack event will be captured, if known. This type of meta-data could aid in the identification of trends and patterns by police investigators overtime.

4.2 Attacker

An *Attacker* is an entity that attempts to or commits a cyber *Attack_Event* to achieve an *Objective*. Donalds and Osei-Bryson [7] classified *Attackers* into the following groups: *Corporate Raider*; *Hacktivist, Political Activist*; *Script Kiddie, Newbie, Novice*; *Cyberpunk, Coder, Writer*; *Insider, User Malcontent*; *White Hat Hacker, Old Guard, Sneaker*; *Black Hat Hacker, Professional, Elite*; *Cyber Terrorist, Cyber Warrior, Information Warrior*; *Digital Pirate, Copyright Infringer*; *Online Sex Offender, Cyber Predator, Pedophile*. We have mostly adopted this classification and have also extended same to include *Unknown Attacker* and *Group Attacker*. The *Attacker* in a cyber *Attack_Event* may be unknown to the *Victim* and the *Attack_Event* may also be committed by a group, therefore their inclusion. Attack_Events committed by individuals are accounted for in the other adopted categories [7].

4.3 Objective

An *Objective* can be considered as the primary driving force why an *Attacker* commits the cyber *Attack_Event.* We have adopted/adapted and extended prior works on the classification of *Objective* [7] to include the following: *Curiosity, Challenge, Thrill*; *Political*, *Ideological*, *Moral*; *Status*, *Fame-seeking*, *Self-aggrandizement*; *Financial Gain*; *Anger*, *Revenge*; *Sexual Impulses*.

4.4 Victim

A *Victim* is an entity that is affected in some way by a cyber *Attack_Event*. Victims could be individuals, groups, organizations and government entities. A *Victim* may be the same as or differ from a *Target*. A *Victim* could be specifically targeted, and, would be the same as the *Target* in such an instance. However, when a *Victim* is affected by a virus that is mass distributed, for example, the *Victim* is not necessarily the specific *Target* but is affected due to a weakness or weaknesses exploited in the system.

4.5 Target

A *Target* can be described as an entity towards which the cyber *Attack_Event* is directed. Infrastructure, organization, state, target individual [4], personal computer, network infrastructure device, server and industrial equipment [14] are proposed as types of *Target*. In this study a *Target* can be of type *Infrastructure*, *Personal Device*, *Network Device*, *Site*, *Organization*, *Government*, *Group* and *TargetIndividual*.

4.6 Impact

An *Impact* can be described as the direct effect of a cyber *Attack_Event* on a *Victim*. Researchers propose differing categories for *Impact*. For instance Kjaerland [16] classifies *Impact* as *Disrupt*, *Distort*, *Destrust*, *Disclosure* and *Unknown* while Simmons et al. [9] propose two broad categories: *Operational Impact* and *Informational Impact*.

They further sub-divide *Informational Impact* into categories *Distort*, *Disrupt*, *Destruct*, *Disclosure* and *Discovery*, while *Operational Impact* is subdivided into categories such as *Installed Malware*, *Denial of Service* and *Web Compromise*. In this study we adopt the *Informational Impact* category proposed by Simmons et al. [9] with the values proposed by Kjaerland [16], which we also extend to include *Discovery* and *UnknownImpact*. Since Simmons et al.'s [9] *Operational Impact* values, in general, identify actions perpetrated in a cybercrime and is covered by our *Attack_Event* concept, we exclude this category. We also include the class *Psychological Impact* [4]. Examples of *Psychological Impact* are *fear*, *reputational damage*, *anxiety*, *depression* and *loss of trust*.

4.7 Location

Location refers to where (i.e., country generally or specific address) the cyber *Attack_Event* occurs. Location has been classified as either *Physical Location* or *Cyberspace* [4]. Additionally, *Location* refers to the country or specific address of the *Victim* that experiences the cyber *Attack_Event*. We note however, that while it may be possible to identify the *Location* from where a cyber *Attack_Event* occurs, this may not correspond to the actual *Location* of the *Attacker* and that a cyber *Attack_Event* via the Internet could be launched from multiple sources.

4.8 Tool and Technique

Tool and Technique can be thought of as the method(s) employed by the *Attacker* in a cyber *Attack_Event*. The categories proposed by Donalds and Osei-Bryson [7] are adopted in this study and are: *Attack Vector* (such as viruses, worms and malware); *Tool* (such as packet sniffers/injectors, password generators and key loggers); *Illicit Collusion* (a term used to describe parties willing to exploit network technology for illicit activities such as communication or data distribution and could include peer-to-peer data sharing, email and Internet Relay Chat (IRC)); and *Social Engineering* (such as impersonation, email and phising). We note that an *Attacker* may use multiple methods in a cyber *Attack_Event*.

4.9 Vulnerability

A *Vulnerability* can be described as a weakness or weaknesses in the system exploited by an *Attacker* in a cyber *Attack_Event*. Therefore, *Vulnerability* is only applicable to Attack_Events committed against ICTs. We adopt the categories of *Vulnerability* proposed by Howard [21]: *Implementation Vulnerability*, *Design Vulnerability* and *Configuration Vulnerability*.

4.10 Offence

An *Offence* can be described as a cyber *Attack _Event* that has been perpetrated by an *Attacker* against a *Victim* that is punishable by law. *Offence* often vary by jurisdiction; examples of *Offence* in the developing country for which this ontology is being developed include: Access with intent to commit or facilitate commission of offence; Computer related fraud or forgery; and, Unlawfully making available devices or data for commission of offence.

5 Ontological Representation and Cybercrime Classification

In this section we present our cybercrime classification ontology (CCO), implemented in Protégé OWL, as well as demonstrate the CCO by using it to classify an actual cybercrime event.

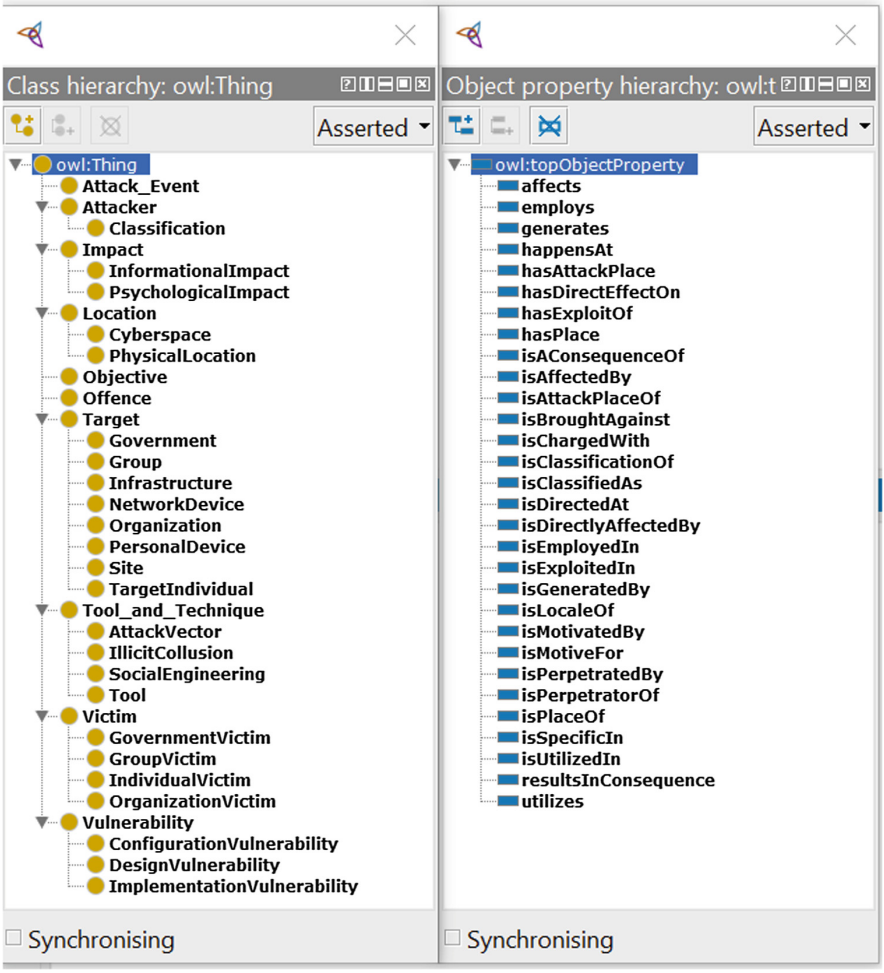

Fig. 2. Classes and properties in the cybercrime classification ontology.

Figure 2 shows the ontological representation of our CCO. This step translates the conceptual model developed from the previous stage (see Fig. 1) to an ontology– based representation using Protégé OWL. Protégé OWL (http://protege.stanford.edu/) is a tool that supports the development of a formal ontology and can be used to model domain concepts as well as the construction of a knowledge-based application, one of our future goals. The OWL ontology typically includes classes along with their descriptions, properties, instances as well as role restrictions. Examples of classes in our CCO includes Attack_Event, Attacker, Victim, Tool_and_Technique. Object properties are used to link two instances together. For instance the property is Charged With links Ronald Oates the instance unauthorised access. Our CCO then is the explicit formal specification of the terms for cybercrime classification (respresented as classes) and the relationships among them.

To demonstrate the artifact, we classify an actual cybercrime using our CCO. The actual cybercrime information is obtained from the print media in a developing country, Jamaica. The case scenario, outlined below, is a synopsis of the cybercrime details printed in two newspapers. Using said details, we instantiate our ontology by adding individuals or instances of classes as appropriate. Subsequently, we demonstrate how the ontology is applied to classify the actual cybercrime. Lastly, we use the DL Query tool in Protégé OWL to query the ontology.

5.1 Actual Cybercrime Synopsis: – Emails Hacked: Nude Photographs Uploaded [22, 23]

The police, on Monday August 27, 2012 arrested and charged a 27-year-old man, Ronald Oates, of a Kingston address, with unauthorised access, unauthorised obstruction and unlawfully making available data for the commission of an offence, all under the Jamaican Cyber Crime Act.

It is alleged that Mr. Oates hacked into the email accounts of his victims, gaining access to their nude photographs. He would then contact the women threatening to upload the photographs to a local website, if he is not paid a certain sum of money, or he would upload the photos and then demand money for them to be removed from the website.

According to the police, Mr. Oates often demanded between $10,000 and $20,000 from his victims, which has amounted to some $150,000 in total. Police say those targeted were mainly from Kingston and St. Andrew and St. Catherine, but the crime also stretched as far as Manchester.

The arrest of alleged computer hacker Ronald Oates has provided some measure of relief for popular entertainer Denyque. Denyque, who was one of the first women to come forward with claims that she was being extorted by the operators of a website that had obtained nude pictures of her, is also appealing to other victims to come forward.

Bianca Bartley owner and designer of a popular jewelry line Peace-is-of-Bianca, is one of the complainants in the matter involving Ronald Oates. Bianca reported that the passwords to her two email accounts were changed without her consent, preventing her from accessing same. Her nude photographs were published on the sites: “Jamiaca-girlsexposed.blogspot.com” (created by the accused), “myfreeblack.com” and “jcan-girls.blogspot.com”.

5.2 Applying CCO to Classify an Actual Cybercrime

How can the CCO shown in Fig. 2 be used to classify the cybercrime presented in the scenario above? To do this we ask a series of questions and create individuals/instances of the appropriate class/classes. Table 2 illustrates the questions and the individuals created along with their classes. Further, we use the class hierarchical structure in our ontology model in Protégé and the conceptual model together to classify and store the cybercrime.

Table 2. Cybercrime classification questions and individuals.

Question	Instance	Class/subclass
What action/cybercrime has been committed?	Emails hacked: nude photos uploaded	Attack_Event
What entity perpetrated the action/cybercrime?	Ronald Oates	Attacker
What is the main motive of the perpetrator?	Financial gain	Objective
How is the perpetrator classified?	Black hat, professional, elite	Classification
What entity was affected by the action/cybercrime?	Bianca Bartley and Denyque	Victim
What is the type of entity affected by the action/cybercrime?	Bianca Bartley and Denyque	IndividualVictim
What entity was the action/cybercrime directed at?	Bianca Bartley and Denyque	Target
What is the type of entity that the action/cybercrime was directed at?	Bianca Bartley and Denyque	TargetIndividual
What effect did the action/cybercrime have on the entity?	Reputational damage Disclosure	PsychologicalImpact InformationalImpact
Where did the action/cybercrime take place as reported by the affected entity?	Social networking site	Cyberspace
What method did the perpetrator use in the action/cybercrime?	Social networking	SocialEngineering

5.3 Querying and Searching the CCO

An important feature of the ontology is the retrieval of results. The DL Query tab in Protégé provides an interface for searching and querying the ontology. Of note, the ontology must be classified by a reasoner before it can be queried in the DL Query tab. Below are examples of queries that can be performed on the CCO.

Q1: "Which attackers used social engineering as a tool/technique in committing a cybercrime?" The result is shown in Fig. 3.

Q2: "Which cybercrimes were committed and resulted in offence(s) being brought against an attacker?" The result is shown in Fig. 4.

Q3: "Which victim was affected by a specific cybercrime [for instance "Emails Hacked: Nude Photos Uploaded"] and has been impacted by same?" The result is shown in Fig. 5.

Q4: "Which cybercrime and attacker are motivated by financial gain?" The result is shown in Fig. 6.

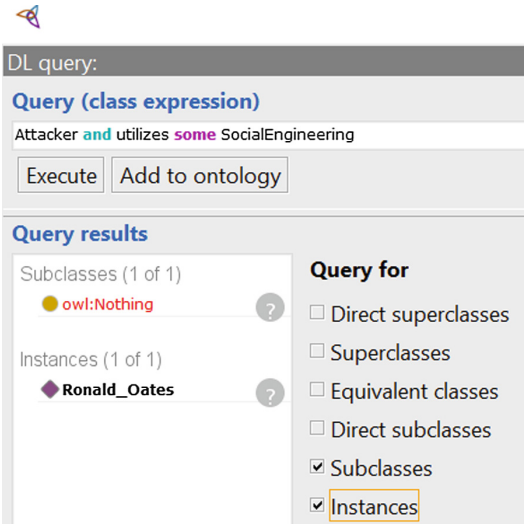

Fig. 3. Attacker using social engineering technique.

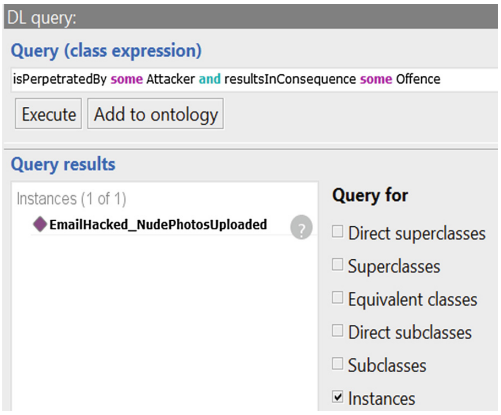

Fig. 4. Cybercrime resulting in offences brought against an attacker.

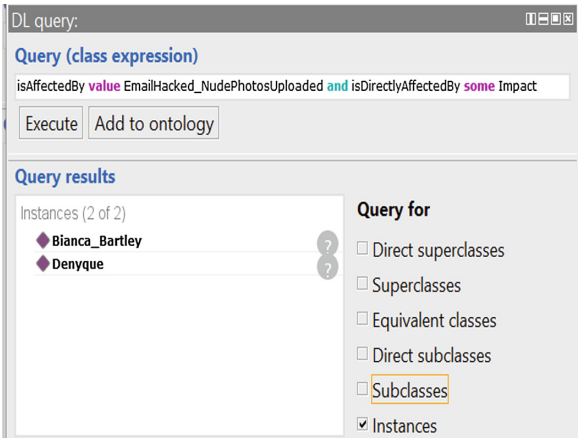

Fig. 5. Victim impacted by specific cybercrime.

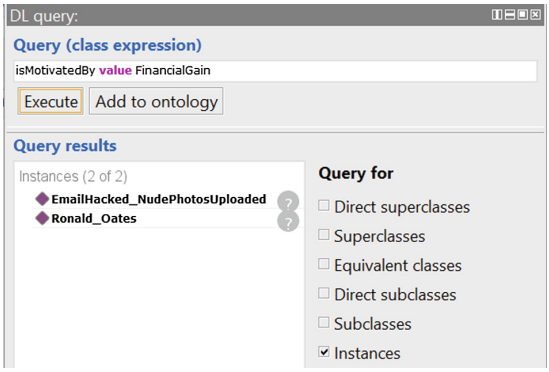

Fig. 6. Cybercrime and attacker motivated by financial gain.

6 Conclusion and Future Work

While few cybercrime classification schemes exist, they are largely incompatible. Further, their focus is generally narrow, concentrating on a single perspective, such as *attacker*, *defender* or *role of the computer*, or they use different terminologies, even though they refer to the same thing. This makes consistent and holistic classification unlikely.

To achieve repeatable and consistent classifications, their needs to be a shared conceptualization of cybercrimes, i.e., an ontology for cybercrime classification. This ontology will provide a common, consistent language that can be used by all cybercrime stakeholders. Without which, the same cybercrime may be classified differently by investigators and can result in inaccurate identification of cybercrime trends and patterns; prerequisites for better allocation of resources to combat cybercrimes. A most salient consideration, especially given the resource constraints that generally confront developing countries.

In this paper we propose an ontology to improve the classification of cybercrimes, CCO. This ontology is an improvement over existing works in several areas: (1) it utilizes a characteristic structure with which to classify cybercrimes; i.e., it classifies properties about cybercrime and not the cybercrime itself; (2) because of its classification structure, it is easily extendable with new terms and concepts and is better able to handle existing and future cybercrimes; and (3) it incorporates varying cybercrime perspectives, enabling a more holistic scheme with which to classify cybercrimes. The demonstration of our ontology also supports the claim that it is an improved classification scheme; we showed how it can be applied to classify a cybercrime from multiple perspectives (including *Attacker*, *Victim*, *Impact*, *Objective*, et al.).

While the artifact is designed to address cybercrime classification in a developing context, we note that it can also be applied to the developed context. Generally, there are many country specific reporting mechanisms of cyber incidents and not enough coordination between them [16]. Our study has, however, provided a formal ontology that may enable improved cybercrime threat assessments if cybercrime information is standardized and shared across jurisdictions. In future we intend to formally evaluate the artifact by implementing same in a developing country police organization. The evaluation would be mainly based on testing the functionality of the artifact to adequately classify cybercrimes reported to the police organization's CSIRT.

References

1. Accenture: 2017 Cost of Cyber Crime Study. Ponemon Institute LLC and Accenture (2017)
2. Caricom Caribbean Community. https://caricom.org/communications/view/caribbean-to-tackle-escalating-cybercrime-with-regional-approach. Accessed 17 Mar 2017
3. Organization of American States (OAS) & Symantec. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf. Accessed 17 Feb 2015
4. Barn, R., Barn, B.: An ontological representation of a taxonomy for cybercrime. In: 24th European Conference on Information Systems (ECIS), İstanbul, Turkey (2016)
5. Ngo, F., Jaishankar, K.: Commemorating a decade in existence of the international journal of cyber criminology: a research agenda to advance the scholarship on cyber crime. Int. J. Cyber Criminol. **11**(1), 1–9 (2017)
6. Stabek, A., Brown, S., Watters, P.A.: The case for a consistent cyberscam classification framework (CCCF). In: Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, UIC-ATC 2009, Brisbane, Australia (2009)
7. Donalds, C., Osei-Bryson, K.-M.: A cybercrime taxonomy: case of the Jamaican jurisdiction. In: CONF-IRM 2014 Proceedings, p. 5 (2014)
8. Land, L., Smith, S., Winchester, D., Pang, V.: The construction of identity offences taxonomy: an Australian context. In: 25th Australasian Conference on Information Systems, Auckland, New Zealand (2014)
9. Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q.: AVOIDIT: a cyber attack taxonomy. Technical report: CS-09-003, University of Memphis (2009)
10. Gruber, T.R.: Toward principles for the design of ontologies used for knowledge sharing. Int. J. Hum.-Comput. Stud. **43**(5–6), 907–928 (1995)

11. Noy, N.F., McGuinness, D.L.: Ontology development 101: a guide to creating your first ontology. Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880, vol. 15, p. 25, Stanford, CA (2001)
12. Staab, S., Studer, R., Schnurr, H.-P., Sure, Y.: Knowledge processes and ontologies. IEEE Intell. Syst. **16**(1), 26–34 (2001)
13. Undercoffer, J., Pinkston, J., Joshi, A., Finin, T.: A target-centric ontology for intrusion detection. In: IJCAI-2003 Workshop on Ontologies and Distributed Systems, pp. 47–58 (2004)
14. van Herdeen, R., Irwin, B., Burke, I.D., Leenen, L.: A computer network attack taxonomy and ontology. Int. J. Cyber Warfare Terrorism **2**, 12–25 (2012)
15. Council of Europe.: Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Accessed 20 July 2012
16. Kjaerland, M.: A taxonomy and comparison of computer security incidents from the commercial and government sectors. Comput. Secur. **25**(7), 522–538 (2005)
17. Simon, H.: The Sciences of Artificial. MIT Press, Cambridge (1996)
18. Hevner, A.R., March, S.T., Park, J.: Design science in information systems research. MIS Q. **28**(1), 75–105 (2004)
19. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. J. Manag. Inf. Syst. **24**(3), 45–78 (2007)
20. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS Q. **37**(2), 337–355 (2013)
21. Howard, J.D.: An analysis of security incidents on the Internet 1989–1995. Engineering and Public Policy, Doctor of Philosophy, pp. 1–319. Carnegie Melon University, Pittsburg (1997)
22. Jamaica Information Service: COPS Make Major Breakthrough in Cybercrime. JIS Service. http://jis.gov.jm/cops-make-major-breakthrough-in-cybercrime/. Accessed 6 Dec 2016
23. The Gleaner: Denyque Praises Cops On Porn Hacker Case. http://jamaica-gleaner.com/gleaner/20120905/lead/lead6.html. Accessed 6 Dec 2016