Classifying Cyber Threat Actors Using an Ontological Approach

Courtney Falk
Ontological Semantic Technology Laboratory
Texas A&M University - Commerce
Commerce, Texas, USA
ontology@tamuc.edu

Tatiana Ringenberg
Computer and Information Technology
Purdue University
West Lafayette, Indiana, USA
tringenb@purdue.edu

***Abstract*—Threat intelligence is a useful tool for organizations looking to build a more proactive information security posture. In threat intelligence, the belligerent party is referred to as the "threat actor." Organizations can anticipate threats and prepare for cyber attacks by understanding the different types of threat actors. A problem with this approach is how organizations define and classify threat actors. The most basic approaches to classifying threat actors are lists of mutually exclusive categories. This paper proposes a way to define cyber threat actors that are more descriptive and flexible than list-based approaches. By describing threat actors using formalisms used in ontology engineering, the result is a scalable, generative approach.**

***Index Terms*—threat intelligence, threat actor, ontology, hacktivism, espionage**

I. Introduction

Cyber threat actors are the persons or organizations behind cyber attacks [1]. Prominent breaches in recent years have elevated threat actors to near celebrity status. News articles about Anonymous, Guccifer, or the Armada Collective are seen in mainstream publications and blogs. Lizard Squad and The Dark Overlord taunt their victims via Twitter [2], [3]. The field of cyber threat intelligence works to understand these and other threat actors. Understanding threat actors benefits organizations with proactive security postures.

Several companies offer cyber threat intelligence products or services. Each company has its own variation of a cyber threat actor classification system. And while there is little universal agreement on what constitutes an adequate classification system, every system wants to pigeonhole a threat actor into one of a small, fixed set of classes.

This paper aims to provide a better system for classifying and describing cyber threat actors. The proposed approach is to replace a static, enumerative system with a flexible, generative system based on the logic used to build ontologies. The important takeaways are the logic and decisions used to define classes of threat actors. Building an ontology-based application is not the goal of this paper, but such an effort could be built using the processes described herein.

II. Prior Work

For organizations, security is no longer a luxury or of secondary importance. Having good security practices is integral to running successful enterprises from banks to non-governmental organizations. Organizations tend to follow a process of increasing maturity in their information security practices. The first stage of information security maturity is the awareness of knowing about threats and vulnerabilities. Second, is the reactive stage when an organization is capable of detecting security breaches and making corrections after the fact. Third, is the proactive stage where organizations spend resources investigating and researching potential threats before they occur.

A. Threat Intelligence

Cyber threat intelligence is one part of a proactive information security posture. Threat intelligence aims to answer the six wh-questions of a computer breach: who, what, when, where, how, and why? What and when are the starting points. A breach is recognized by an affected device, which in turn offers forensic information as to when it happened. The what and when may expand in scope as an incident response investigation proceeds. Four years after LinkedIn suffered a data breach they were forced to re-examine the size and scope in light of additional data disclosures [4].

There are two ends of the where question; where the attack originated and where the target was located. The latter location should be readily available from the affected organization the same as the what and when information. An originating location for the attack is more difficult to ascertain. Hackers can compromise computers all across the world. A basic operations security (OPSEC) measure is to route an attack through a compromised intermediary. An OPSEC-savvy hacker would avoid attacking from his/her home at A directly against target B, instead opting to route all traffic through a victim at C. Attacks can involve three or more different nations with only a modest increase in complexity for the attacker.

The final two wh-questions that threat intelligence addresses are the who and the why. Who actually conducted the attack, and why did they set out to do so? These are arguably the most difficult questions to answer because they imply a level of attribution, and attribution is a complex and difficult task to perform [5], [6]. Incident remediation firm Mandiant went into fine-grained attribution detail with their *APT1* report [7]. But this level of attribution is the exception and not the rule.

Threat analysts looked for a way to help answer the who and why questions in the face of ambiguous or otherwise missing information. One tool that was developed was the classification system for a cyber threat actor. Such a system defines a set of classes along with associated properties for members of those classes. Analysts assign threat actors to the category that best matches the information that is found in an investigation.

At least two different approaches to classifying threat actors exist. The first approach, examining an actor's actions and motivations, is the basis for this paper. The second approach is classifying a threat actor based on the tools, techniques, and procedures (TTP) that they utilize in a breach, the term 'TTP' itself deriving from a related military definition [8]. The TTP-based approach looks to leverage the information a threat analyst is most likely to have; the what and the when. But this approach is self-limiting. Take, for example, advanced persistent threats (APTs). No single definition for what qualifies as an APT exists, but many such definitions talk about TTP that focus on a long-term, stealthy presence inside a victim's computer network. But this makes assumptions about the attacker's OPSEC. Furthermore, it begs the very definition of what 'advanced' is [9]. Sometimes an attacker may want to hide in the noise of the greater Internet. If threat analysts see an attacker using commodity, off-the-shelf malware like Poison Ivy or Zeus then that may lead them to conclusions that the attacker is attacking as many targets as broadly as possible, when in reality the attacker is targeting that organization specifically and didn't want to lose their bespoke malware and zero-day exploits on initial surveillance.

There are benefits to such systems. Not every organization can monitor every threat in the world. But thinking critically about threat actors lets an organization anticipate and prepare for attacks. As an example, a petroleum drilling company wants to initiate an exploratory well in a new nation. By virtue of their involvement with the environment, the drilling company monitors threat actor groups that espouse eco-friendly viewpoints. Also, awareness of the geopolitical environment in and concerning the new nation can inform the company about what nation-state actors might want access to their proprietary information.

B. Threat Actor Categorization

Table I is a comparison of the different classes that information security companies use. Notice how three of the eight categories feature almost universal inclusion while the remaining five categories are sparsely represented.

The definitions for the threat actor categories are summed up as follows:

1) Criminal - Hacks for money.
2) Ideological, Social - Advocating for a social ideology/-cause.
3) Ideological, Violent - Looking to advance a political position through the use of violence.
4) Nation-State - Hackers working for or on behalf of a national government.

	Recorded Future [10]	Fortinet [11]	SurfWatch [12]	CrowdStrike [13]	SecureWorks [14]	Webroot [15]	ICS-CERT [16]
Criminal	x	x	x	x	x	x	x
Ideological, Social	x	x	x	x	x	x	x
Ideological, Violent			x		x		x
Nation-State	x	x	x	x	x	x	x
Employee, Intentional	x	x			x		
Employee, Unintentional		x					
Anarchists		x	x				x
Corporate					x		x

TABLE I
A COMPARISON OF THREAT ACTOR CATEGORIES. THE THREE MOST COMMON CATEGORIES ARE SHOWN IN BOLDFACE.

5) Employee, Intentional - Existing employee who abuses their trusted access maliciously.
6) Employee, Unintentional - Uninformed or negligent employee.
7) Anarchists - Hacking for fun and/or notoriety.
8) Corporate - Industrial/corporate espionage.

Other interesting trends are found when examining Table I. Only half of the threat actor categorization systems surveyed include internal employees as a factor. And only one of those three makes a meaningful distinction between an employee who willfully violates the organization's computer protections (the 'insider') [17] and an employee whose unintentional mistakes lead to vulnerability. This suggests that most classification systems are concerned only with external threats, and neglect threats of an internal nature.

While every system includes the 'hacktivist,' or ideologically-motivated hacker, half of the systems make a distinction between hacktivist and (cyber)terrorist [18]. However, terrorists are ideologically motivated the same as hacktivists but they are more willing to use violence to bring about this goals. This suggests that these companies find violence to be a distinguishing characteristic between ordinary hacktivists and the more extreme terrorists.

C. Lazarus Group

Why is this list-based approach problematic? The real-world example of the Lazarus group highlights problems of enumerative threat actor classification. One possible attribution for Lazarus is Unit 180 of the North Korean Reconnaissance General Bureau intelligence agency [19]. We will set aside the difficulties of correct attribution that were discussed earlier in this paper and make the assumption that Lazarus is indeed a part of the North Korean government for the sake of example.

Now we will examine some of the campaigns and attacks attributed to Lazarus, starting with the breach at Sony Motion Pictures. The Sony attack occurred shortly before the planned release of the buddy stoner comedy, *The Interview* [20]. *The Interview* tells the story of a self-absorbed celebrity interviewer who seeks to validate his journalistic bona fides by

interviewing the leader of North Korean, Kim Jong-Un [21]. A comedy, the film portrays a fictionalized yet unflattering portrait of the North Korean head of state.

Hackers identifying themselves as the Guardians of Peace broke into Sony computer networks, vandalized web pages, and stole data such as internal email communication. The emails were eventually leaked publicly, embarrassing studio executives [22]. The motivation behind the Sony attack is apparently nationalistic. Using the kind categories of Table I, this kind of attacker would be classified as a Social Ideological hacker. But the so-called Guardians of the Peace were eventually identified as being the same as the Lazarus group [23].

Jump ahead three year to 2017. In a complex series of events, a Windows exploit attributed to the United States National Security Agency was packaged with ransomware and released as a worm [24]. This WannaCry worm rapidly spread across the globe and disrupted logistics firms, hospitals, and even pet food manufacturers. The WannaCry worm and its ransomware demanded money for the safe return of the affected data, an act of criminal extortion. But the ransom money sat uncollected for four months before vanishing [25]. As with the Sony case, attribution linked the attack to the Lazarus group.

Now the difficulty in using the categories seen in Table I are apparent. We began with the conception of Lazarus being a nation-state actor. But the Sony attack demonstrated an ideological bent, and the WannaCry campaign was arguably criminal in nature. So is Lazarus some combination of all three of these categories? How can the existing classification systems handle this type of situation.

D. Taxonomies, Typologies, and Ontologies

The flat classification systems already examined are insufficient to adequately explain the different categories of cyber threat actors. Approaches with more structure to them include taxonomies, typologies, and ontologies.

Taxonomies offer a possible solution. A taxonomy is a tree-like structure used for organizing classes of objects. By taking the classes, and arranging them into a hierarchy along with abstract classes to organize them, the result looks like Figure 1.

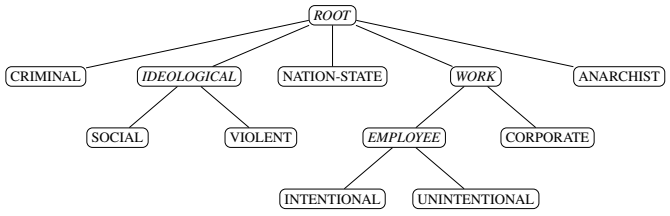

Fig. 1. Classes from Table I structured into a taxonomy.

Problems arise with using taxonomies for the cyber threat actor classes. Just as in the flat classification systems, membership is the class is an identity commitment; the class is critical to the identity of the hacker, and a hacker can only belong to one of the classes. So if a hacker is placed in the Criminal category then being a criminal hacker is core to his/her identity, and he/she can't ever belong to a different class because that would change the hacker's core identity.

Whereas taxonomies impose a hierarchical structure, typologies take a bottom-up approach, defining categories based on common features [26]. The downside of typologies is their brittleness. If a new feature is introduced then it could break the way that the current set of categories are defined, necessitating a new set of categories altogether.

Ontologies exist in several variations. Some ontologies have computational properties built into them to enable efficient processing [27]. Other ontologies focus instead on modeling the ambiguity of natural language [28]. What these different ontologies have in common is their ability to represent knowledge.

An ontology incorporates a taxonomy like a skeleton. The taxonomic structure defines how the concepts in the ontology are related [29]. What an ontology adds are meaningful relations between the concepts. These meaningful relations allow an ontology to define knowledge with more nuance than by taxonomy alone.

Ontologies are vulnerable to some of the same problems as taxonomies such as multiple inheritance. This is due to ontologies using taxonomies as a base structure. Where ontologies differ is in the semantic relations they include and the different, non-taxonomic types of structures they can produce using those semantic relations.

Work to apply the logic of ontologies to the threat intelligence realm already exists [30]. The work presented in this paper could be treated as a smaller domain of what Falk proposed. Though as noted above, this paper avoids making commitments to any one particular ontology paradigm while Falk was specifically interested in an ontology defined in the Web Ontology Language (OWL) that is utilized in Semantic Web applications [31].

III. An Ontological Approach

Existing approaches to classifying threat actors are based on enumerative lists. Lists are inflexible in that adding new entries can require changing the previous entries.

This section redefines the classes of cyber threat actor shown in Table I in terms of the concepts found in an ontology. Each class-specific section defines one or more frames [32]. The frames are written in the style of Lisp S-expressions popularized in *Ontological Semantics* [28]. Not all the concepts and properties see in the following figures are explicitly defined in this paper. Those that are not can be found in an upper ontology, which is the uppermost general part of an ontology that is useful across multiple application domains [33].

A. Criminal

A convincing argument can be made that all threat actors are criminals. After all, they all intrude into computing systems where they are neither wanted nor invited, and once inside they copy or alter data as they see fit. This argument assumes a universal code of law that doesn't exist.

Criminals (organized and otherwise) are interested in actions that produce financial dividends for themselves. Theft and extortion are the two types of crimes that can be used to classify a criminal threat actor. Theft via cyberspace has a lengthy history. Phishing emails used to be easily identifiable by their requests for bank account information, information that the criminal could use to liquidate the victim's accounts. Cyber extortion has gained attention in recent years with the rise of ransomware attack. Ransomware is a subclass of malware that denies a user access to his/her legitimate files. If the victim pays the ransom then the attacker sometimes grants access to the files [34]. Before the notable WannaCry and NotPetya ransomware attacks of 2017 [35], [36], ransomware infection rates from 2015 through 2016 were maintaining a high average rate [37].

```
(HUMAN
   (AGENT–OF (SEM (HACK
      (THEME (SEM (STEAL EXTORT)))
   )))
)
```

Fig. 2. Example frame for a criminal hacker.

According to the frame described in Figure 2, a Criminal hacker is someone who hacks in order to then conduct theft and/or extortion. Notice that this definition of a criminal hacker doesn't make any distinction between "organized crime" and disorganized crime. A threat intelligence analyst can define the appropriate subcategories if they so choose.

B. Nation-State

Nation-state actors are the bogeymen of the Internet. They have seemingly limitless resources to include time and skilled hackers. It is said that if a nation-state actor wants you then they'll get to you sooner or later.

There are two different ways that a hacker could be considered a nation-state threat actor. The first and most obvious is to belong as a member to a nation's organization dedicated to offensive cyber actions.

The second way a hacker could be considered a nation-state actor is to hack on behalf, or at the direction of, a nation-state without actually belonging to it or its intelligence organs. This was the case that Clifford Stoll found when stumbled across a network breach at the Lawrence Berkeley National Laboratory [38]; the Soviet government had hired an East German hacker to steal intellectual property for them. These directed attacks may be done voluntarily by patriotically-minded citizens, or the nation-state might coerce groups of known criminals.

This logical division of the Nation-State threat actor gives two subclasses that require different descriptions: Nation-State (Member) as seen in Figure 3, and Nation-State (Directed) as seen in Figured 4. This division creates a non-monotonic case in that while a person belong to any type of organization, a directed nation-state actor, by definition, can not belong to his/her nation's offensive cyber organization.

```
(HUMAN
   (COMPONENT–OF (SEM (GOVERNMENT–AGENCY)))
)
```

Fig. 3. Example frame for a member nation-state hacker.

```
(HUMAN
   (COMPONENT–OF (NOT (GOVERNMENT–AGENCY)))
   (DIRECTED–BY (SEM (GOVERNMENT–AGENCY)))
)
```

Fig. 4. Example frame for a directed nation-state hacker.

IV. Combined Ontological Classes

The expression power of the ontological approach is best demonstrated using some of the more complex real-world examples. Each of these scenarios bridges two or more traditional threat actor categories.

A. Russian Business Network

The Russian Business Network (RBN) was an organization that specialized in "bullet-proof hosting." [39] What bullet-proof hosting is is the online hosting of web sites and other network-based services for illicit purposes. Malware command-and-control, child pornography trading, and the selling of stolen credit cards are all prime clients for a bullet-proof host.

But when the Estonian government offended the Russian government by relocating a monument to the Soviet war dead of WWII, the ensuing distributed denial-of-service (DDoS) originated from RBN-controlled networks **??**. The attribution of the attack to the Russian government will always be somewhat circumstantial, but it will be assumed to be true for this example. The result is seen below in Figured 5.

```
(ORGANIZATION
   (DIRECTED–BY (SEM
      (INTELLIGENCE–AGENCY)))
   (COMPONENT–OF (VALUE (NONE)))
   (AGENT–OF (SEM (DDOS)))
   (SELLS (SEM (BULLET–PROOF–HOSTING)))
)
```

Fig. 5. The Russian Business Network.

The ⟨AGENT-OF, DDOS⟩ and ⟨SELLS, BULLET-PROOF-HOSTING⟩ tuples come from the criminal nature of RBN's activities. The ⟨DIRECTED-BY, INTELLIGENCE-AGENCY⟩ and ⟨COMPONENT-OF, NONE⟩ come directly from the Figure 4 example of a directed nation-state actor. The

resulting frame connects the RBN organization to activities that might classify it as a criminal threat actor, and with the kind of partner organizations that might classify it as a nation-state actor. In this scenario, the use of an ontological approach captures these different attributes in a single place.

B. Lazarus, Revisited

Now that the classes of threat actors are redefined using an ontology, it is a good time to re-examine the Lazarus group and see if the ontological approach provides an improved definition. Figure 6 below combines aspects of Figures 2 and 3:

```
(ORGANIZATION
   (COMPONENT–OF  (SEM
      (INTELLIGENCE–AGENCY)))
   (FOLLOWS–SYSTEM  (SEM
      (POLITICAL–BELIEF–SYSTEM)))
   (AGENT–OF  (SEM  (HACK)))
   (THEME  (SEM  (STEAL EXTORT)))
)
```

Fig. 6. Lazarus group revisited.

The ⟨COMPONENT-OF, INTELLIGENCE-AGENCY⟩ tuple identifies Lazarus as being nation-state. The original frame for a nation-state hacker in Figure 3 expects a ⟨COMPONENT-OF, INTELLIGENCE-AGENCY⟩ tuple, but the INTELLIGENCE-AGENCY concept is a subclass of GOVERNMENT-AGENCY and therefore satisfies the same requirements. Ideological hackers contribute the second tuple, ⟨FOLLOWS-SYSTEM, POLITICAL-BELIEF-SYSTEM⟩. POLITICAL-BELIEF-SYSTEM being a subclass of BELIEF-SYSTEM. More specific to the North Korean scenario, the political belief system would need to describe the DRPK's Juche system of self-reliance [40]. The final part of the frame in Figure 6 is an nested event, HACK. This description of HACK comes from the criminal hacker in Figure 2.

All three of the component classes come together to form a single, coherent picture of the Lazarus group cyber threat actor. The final result is far more expressive than what was seen in either the flat classification systems nor the taxonomic approach. Furthermore, this ontological approach is generative and capable of describing novel classes of threat actor that haven't yet been identified by threat intelligence professionals.

V. Conclusion

This paper began by exploring current approaches to classifying cyber threat actors. These systems are flat and enumerative. Extending such a flat system into a hierarchical taxonomy gains some expressive power yet fails to solve the problem of mutual exclusivity between threat actor classes. Furthermore, the taxonomic approach brings with it new logical challenges.

Ontological approaches produce flexible and generative classification systems. Such an ontology-based system allows for finer-grained reporting by threat intelligence analysts. Analysts are no longer forced to choose the threat actor category that is the least wrong, and can instead describe the threat actor accurately and correctly.

Finally, the ontological system of classifying threat actors was applied to the real-world scenario presented by the Russian Business Network and the Lazarus group of hackers. These examples demonstrate the application of three different kinds of logical relations used when describing concepts within an ontology:

- Structural parts/wholes of objects.
- Roles played within an event.
- Semantic relations between objects.

Ontologies provide flexible and expressive tools for representing the world as it exists. Threat intelligence can be improved in terms of quality and accuracy through the use of ontologies, and this paper describes one such application.

Acknowledgment

The authors would like to thank the Optiv corporation, and specifically Mr. Danny Pickens, for the opportunity to work on problems of applied threat intelligence.

References

[1] M. Haber, "What is the difference between a threat actor, hacker and attacker?" *BeyondTrust*, May 2017. [Online]. Available: https://www.beyondtrust.com/blog/difference-between-a-threat-actor-hacker-attacker/

[2] S. Pudwell, "Latest lizard squad twitter hack illustrates the lucrative potential of ddos attacks," *ITProPortal*, January 2015. [Online]. Available: https://www.itproportal.com/2015/01/30/latest-lizard-squad-hack-shows-increasing-strength-ddos-attacks/

[3] J. Roettgers, "Twitter bans account of orange is the new black hacker the dark overlord," *Variety*, June 2017. [Online]. Available: https://variety.com/2017/digital/news/dark-overlord-twitter-suspended-1202477610/

[4] B. Krebs, "As scope of 2012 breach expands, LinkedIn to again reset passwords for some users," May 2016. [Online]. Available: https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/

[5] J. Healey, "Beyond attribution: Seeking national responsibility for cyber attacks," January 2012.

[6] T. Rid and B. Buchanan, "Attributing cyber attacks," *The Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015.

[7] Mandiant, "APT1: Exposing one of China's cyber espionage units," February 2013. [Online]. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[8] "Department of defense dictionary of military and associated terms," November 2010.

[9] R. M. Lee, "Common analyst mistakes and claims of energy company targeting malware," July 2016. [Online]. Available: http://www.robertmlee.org/common-analyst-mistakes-and-claims-of-energy-company-targeting-malware/

[10] RFSID, "Proactive defense: understanding the main threat actor types," August 2016. [Online]. Available: https://www.recordedfuture.com/threat-actor-types/

[11] A. Giandomenico, "Byline: Know your enemy: Understanding threat actors," July 2017. [Online]. Available: https://blog.fortinet.com/2017/07/13/byline-know-your-enemy-understanding-threat-actors

[12] SurfWatch Labs, "Cyber threat categories." [Online]. Available: https://www.surfwatchlabs.com/threat-categories

[13] A. Meyers, "Meet the adversaries," September 2014. [Online]. Available: https://www.crowdstrike.com/blog/meet-the-adversaries/

[14] SecureWorks, May 2017. [Online]. Available: https://www.secureworks.com/blog/cyber-threat-basics

[15] Webroot Blog Staff, "Cyber threat actors," February 2016. [Online]. Available: https://www.webroot.com/blog/2016/02/23/cyber-threat-actors/

[16] L. K. Gershwin, "Statement for the record for the joint economic committee cyber threat trends and US network security," June 2001. [Online]. Available: https://www.cia.gov/news-information/speeches-testimony/2001/gershwin_speech_06222001.html

[17] M. Bishop and C. Gates, "Defining the insider threat," in *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*. ACM, 2008, p. 15.

[18] D. E. Denning, "Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy," *Networks and netwars: The future of terror, crime, and militancy*, vol. 239, p. 288, 2001.

[19] J. Park and J. Pearson, "Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West," *Reuters*, May 2017. [Online]. Available: http://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020

[20] L. Grisham, "Timeline: North Korea and the Sony Pictures hack," *USA Today*, December 2014. [Online]. Available: https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/#

[21] E. Goldberg and S. Rogan, "The interview," Sony Motion Pictures, 2014.

[22] WikiLeaks, "Sony," April 2015. [Online]. Available: https://wikileaks.org/sony/press/

[23] A. Peterson and E. Nakashima, "The hackers that took down Sony Pictures are still on the attack, researchers say," *Washington Post*, February 2016. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2016/02/24/the-hackers-that-took-down-sony-pictures-are-still-on-the-attack-researchers-say/

[24] A. Islam, N. Oppenheim, and W. Thomas, "SMB exploited: WannaCry use of "Eternalblue"," May 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

[25] S. Larson, "Someone has emptied the ransom accounts from the WannaCry attack," *CNN*, August 2017. [Online]. Available: http://money.cnn.com/2017/08/03/technology/wannacry-bitcoin-ransom-moved/index.html

[26] A. Marradi, "Classification, typology, taxonomy," *Quality and Quantity*, vol. 24, no. 2, pp. 129–157, 1990.

[27] T. Berners-Lee, J. Hendler, O. Lassila *et al.*, "The semantic web," *Scientific American*, vol. 284, no. 5, pp. 28–37, 2001.

[28] S. Nirenburg and V. Raskin, *Ontological semantics*. MIT Press, 2004.

[29] R. J. Brachman, "What IS-A is and isn't: An analysis of taxonomic links in semantic networks," *Computer*, vol. 10, 1983.

[30] C. Falk, "An ontology for threat intelligence," in *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2016, p. 111.

[31] G. Antoniou and F. Van Harmelen, "Web ontology language: OWL," in *Handbook on Ontologies*. Springer, 2004, pp. 67–92.

[32] M. Minsky, "A framework for representing knowledge," in *The Psychology of Computer Vision*. McGraw Hill, 1975, pp. 211–277.

[33] C. Falk, "Infinite Machines upper ontology," September 2017. [Online]. Available: https://www.researchgate.net/publication/320142956_Infinite_Machines_Upper_Ontology

[34] Trend Micro, "Lesson learned from ProtonMail incident: Do not pay cybercriminals," November 2015. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/protonmail-incident-do-not-pay-cybercriminals

[35] B. Krebs, "U.K. hospitals hit in widespread ransomware attack," *KrebsonSecurity*, May 2017. [Online]. Available: https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/

[36] L. Mathews, "The NotPetya ransomware may actually be a devastating cyberweapon," *Forbes*, June 2017. [Online]. Available: https://www.forbes.com/sites/leemathews/2017/06/30/the-notpetya-ransomware-may-actually-be-a-devastating-cyberweapon/#6aef1f839e89

[37] A. Rab, A. Neville, A. Anand, C. Wueest, D. Tan, H. Lau, J. DiMaggio, J. Graziano, L. O'Brien, O. Cox, P. Coogan, S. Meckl, and Y. L. Chong, "An ISTR special report: ransomware and businesses 2016," August 2016. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

[38] C. Stoll, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Simon and Schuster, 2005.

[39] M. Goncharov, "Criminal hideouts for lease: Bulletproof hosting services," *Forward-Looking Threat Research (FTR) Team, A TrendLabsSM Research Paper*, vol. 28, 2015.

[40] C. Armstrong, "Necessary enemies: Anti-Americanism, Juche ideology, and the torturous path to normalization," U.S.-Korea Institute, Working Paper WP 08-3, September 2008.