Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 2 Article 3

February 2022

A Taxonomy of Cyberattacks against Critical Infrastructure

Miloslava Plachkinova
Kennesaw State University, mplachki@kennesaw.edu

Ace Vo
Loyola Marymount University, ace.vo@lmu.edu

A Taxonomy of Cyberattacks against Critical Infrastructure

Abstract

The current study proposes a taxonomy to organize existing knowledge on cybercrimes against critical infrastructure such as power plants, water treatment facilities, dams, and nuclear facilities. Routine Activity Theory is used to inform a three-dimensional taxonomy with the following dimensions: hacker motivation (likely offender), cyber, physical, and cyber-physical components of any cyber-physical system (suitable target), and security (capable guardian). The focus of the study is to develop and evaluate the classification tool using Design Science Research (DSR) methodology. Publicly available data was used to evaluate the utility and usability of the proposed artifact by exploring three possible scenarios – Stuxnet, the Ukrainian power grid shut down, and ransomware attacks. While similar taxonomies exist, none of them have been verified due to the sensitive nature of the data and this would be one of the first empirically validated frameworks to explore cyberattacks against critical infrastructure. By better understanding these attacks, we can be better prepared to prevent and respond to incidents.

Keywords

cybersecurity, critical infrastructure, routine activity theory

INTRODUCTION

Cybercrime is a problem of growing significance in society. This is partially due to the mass integration of technology not just in our everyday lives, but also in critical government infrastructure. The overreliance of technology has created a new opportunity for hackers and other individuals with malicious intentions to take advantage and compromise systems and breach databases with sensitive information that may pertain to national security, individuals' medical, financial, educational, personal, etc. records. When it comes to critical infrastructure such as power plants, nuclear facilities, electric grid, dams, they are especially vulnerable to attacks because they were built predominantly before today's cybersecurity standards. These growing opportunities combined with the increased motivation and resources that hackers have, make our society an easy target of cybercrimes.

Specifically, cyberterrorism and information warfare demonstrate in practice the massive impact of malicious attacks. While such attacks may not be as frequent as other types of cybercrimes like cyberstalking, cyberbullying, identity theft or data breaches, they have the capability to potentially take down entire countries' infrastructures and paralyze critical resources. Such attacks are often state-funded and categorized as Advanced Persistent Threats (APT). Thus, it is vital to focus on this growing threat to national security and consider new approaches to better protect individuals and government structures and identify means to respond to incidents.

A significant first step in this direction would be to analyze the hacker culture and understand why these individuals commit cybercrimes in the first place. Attacking the root cause of the problem is the only viable solution to reduce cybercrimes in the future. While some hackers may be motivated by financial gain, others commit crimes for social or political reasons. By focusing on these different types of offenders, we can propose more adequate solutions to policy makers because one single policy may not be able to adequately resolve all these problems.

PROBLEM IDENTIFICATION

When it comes to cybercrimes, a significant issue is the lack of policies to effectively deter the offenders. This is partially due to the fact that cybercrimes often cross state and national borders and this creates a significant challenge when it comes to identifying and prosecuting the hackers. Furthermore, some countries such as China, Russia, or Ukraine for instance, do not have extradition treaties with the US, which makes it very difficult to prosecute any hackers residing in those countries.

Identifying the hackers who commit cybercrimes is equally challenging. The growing use of technology and the easier access to exploits on the Darknet make it easier even for someone with limited technical skills to commit crimes. And while technology is rapidly developing, our legislature on cybercrimes and cyberterrorism is lagging behind. Part of this is due to the complexity of the topic and the lack of understanding among policy makers. In addition, many still do not believe that entire critical infrastructures can be compromised with little effort. However, just because it has not happened in large scale, it does not mean that such attacks are impossible or unfeasible. The lack of adequate incident response guidelines is another important aspect of this problem.

The challenges of cybercrime and cyberterrorism also come from the fact that we are yet to see a massive attack in the US. However, critical infrastructure in Iran and Ukraine has already been attacked. In 2011, Iran's nuclear program was compromised with the Stuxnet virus and in 2015 Ukraine's power grid experienced a cyberattack. These examples demonstrate the global impact such crimes can have. This is often due to the fact that critical infrastructure has been developed a while ago when technology was not so sophisticated. So, when such legacy information systems, also known as Supervisory Control and Data Acquisition (SCADA), are now connected to the Internet, this creates a myriad of threats. For instance, the legacy systems are no longer maintained and often lack sufficient antivirus protection. These flaws make them easy targets of hackers who are often state-funded and have the resources, time, and opportunities to take down critical systems of national security.

The lack of a unified approach to protect critical infrastructure is another significant problem. There are so many different types of attacks and global organizations and governments fail to even agree on the definitions of "cybercrime" and "cyberterrorism". Most criminological theories predominantly focus on physical crime and not much attention has been paid to explaining and reducing cybercrimes, especially those focused at attacking critical infrastructure and SCADA systems.

BACKGROUND LITERATURE

Cybercrime

Like traditional crime, cybercrime has many different facets and occurs in various environments and scenarios. When it comes to defining the term "cybercrime", there have been multiple attempts and the definition itself evolves over time due to the changes in technology, its growing implementation in society, and the impact of using various tools and devices in our lives. For example, The Council of Europe's Cybercrime Treaty uses the term "Cybercrime" to refer to offences ranging from criminal activity against data to content and copyright infringement (Krone, 2005). However, Zeviar-Geese (1997) suggests that the definition is broader, including activities such as fraud, unauthorized access, child pornography, and cyberstalking. The United Nations Manual on the Prevention and Control of Computer Related Crime (United Nations, 1995) includes fraud, forgery, and unauthorized access in its cybercrime definition. Gordon and Ford (2006) define cybercrime as: "any crime that is facilitated or committed using a computer, network, or hardware device" (p. 14).

The National Research Council (2009) described cyberattacks as "deliberate computer-to-computer attacks that disrupt, disable, destroy, or take over a computer system, or damage or steal the information it contains" (p. 1). The umbrella term "cyberattack" can include any of the following: infecting computers and networks with viruses and worms that control, slow down or damage computers, exploiting spyware to probe for vulnerabilities or steal data, and conducting denial of service attacks, with or without the assistance of botnets, to overwhelm websites and networks by flooding them with junk communications. Cyberattacks exclude physical assaults on computers using other weapons, such as destroying computers with hammers or explosives (Kenney, 2015). According to the National Research Council (2009), cyberattacks are computer attacks on other computers carried out in cyberspace, including the Internet, telecommunications infrastructures, and computer systems. The immediate objective of a cyberattack may be to harm the computer targeted, steal information from it, or simply observe the system to exploit vulnerabilities for a subsequent attack. The key is that the attacker conducts the intrusion with hostile, if not necessarily destructive, intent – without the knowledge or consent of the victim.

However, the problem with all these definitions is that they are very broad and do not contain many discriminating properties to classify them more specifically. This lack of differentiation may also lead to disparities in the potential sentencing procedures when it comes to prosecuting hackers. Furthermore, the perpetrators of cyberattacks can be states or non-state actors, the damage caused by the attack can be extensive or minuscule, and the attack's purpose may be to achieve almost any economic, political, social, or psychological objective (Kenney, 2015).

Cyberterrorism

Cyberterrorism, or cyberwarfare, is much less frequent compared to cybercrimes and cyberattacks. These are typically carried out by entire states who launch repeated computer attacks against their adversaries to deny them the ability to use cyberspace effectively, while safeguarding their own ability to do the same. Such attacks are known as Advanced Persistent Threats (APT). The term "APT" emerged in the last 10 years and it has been associated with a new type of insidious threats that use multiple attack techniques and vectors, and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time (Tankard, 2011).

Cyberwarfare refers to offensive computer assaults that seek to damage or destroy adversaries' networks and infrastructures or deter them from waging cyberattacks of their own. Like conventional warfare, cyberwarfare is instrumental: belligerents seek to impose their will on their enemies by attacking them in pursuit of some political goal or objective (Clausewitz, 1976). Unlike traditional warfare, cyberwarfare occurs exclusively in cyberspace. The physical acts of destroying virtual networks by bombing computer servers or telecommunications cables are now taking place in the cyberspace.

Cyberwarfare is largely, but not exclusively, the domain of states. States, and private hackers that act on their behalf, view cyberwarfare as a tool through which they can advance their national interests. This virtual continuation of policy by other means is still less violent than traditional warfare, leading some observers to declare that cyberwarfare is not "real." In one version of this argument, cyberwar is not real war because cyberweapons lack their "own force or energy" (Rid, 2013, p. 81).

Because information about cyberterrorism and cyberterrorists is generally considered classified and cannot be released to the public, the public can usually only infer that cyberterrorism and cyberterrorists exist. However, in 2010 Federal Bureau of Investigation (FBI) chief, Robert Mueller, told an RSA Conference of computer security professionals, ‘‘The cyber-terrorism threat is real and rapidly expanding’’. He indicated that terrorists have shown a clear interest in hacking skills and combining real attacks with cyberattacks (Hua & Bapna, 2013).

APT is a critical component of cyberterrorist attacks. Tankard (2011) defines the term as “a new breed of insidious threats that use multiple attack techniques and vectors and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time” (p. 16). Furthermore, he explains that traditional defenses aimed at keeping known threats out of the network are no longer sufficient against the exploits being used to conduct such attacks. Tankard (2011) insists that the focus should be on “developing a defense in depth strategy that aims to constantly monitor networks and security controls for their effectiveness” (p. 16). These advanced persistent threats are the main weapon of cyberterrorists and in order to launch such an attack, one must be supported by the infrastructure of an entire country. Since there are not that many powerful countries in the world in terms of their cyber capabilities, it could be easy to identify the offenders based on the current socio-political context in the world because often these crimes are triggered by certain political and economic events. However, proving beyond reasonable doubt in front of an international court that a particular country committed the crime is essentially impossible.

Hacker Motivation

Generally, cyberterrorists are considered a subgroup of hackers (Beveren, 2001; Rogers, 1999). What differentiates them from hackers is their motivation. Typically, cyberterrorists are politically or religiously motivated and similar to the examples we have seen in the physical world – their goal is to create fear and panic among civilians and disrupt or destroy public and private infrastructure (Hua & Bapna, 2013).

Sometimes cyberterrorists may also try to coerce a targeted government to negotiate with them, or show their existence to their community, or demonstrate their capabilities to their political and financial supporters (Embar-Seddon, 2002; Verton & Brownlow, 2003). Furthermore, as Poremba (2011) points out, "Unlike viruses or computer attacks that result in a denial of service a cyberterrorist attack is designed to cause physical violence or extreme financial harm". In contrast, common hackers' motivations include addiction to hacking, curiosity, intention to gain power, peer recognition and the sense of belonging to a group (Beveren, 2001). Increasingly, the motivation is to make money (Aaronson, 2005) and some cases from the U.S. Department of Justice are showing that most hackers tried to make money from their hacking (Hua & Bapna, 2013). Generally, a skilled hacker may attack the same target as a cyberterrorist; however, the cyberterrorist would typically have more resources than the hacker to support long-term uninterrupted attacks or APTs (Furnell & Warren, 1999; Quigley, 2007). This evidence only comes to show the growing impact of cyberterrorism on our society and the pressing need to develop new policies that would provide international law enforcement agencies with the necessary legal frameworks to investigate and prosecute cybercrimes and cyberterrorism.

When it comes to the motivation of any cybercriminals, there are three basic aspects. They could be inspired by the political, socio-cultural, or economical contexts. Gandhi et al. (2011) describe this phenomenon as a Venn diagram, and they provide examples of each type of hacker motivation.

Cyber criminals involved in politically motivated attacks can be members of extremist groups who use cyberspace to spread propaganda, attack websites and networks of their political enemies, steal money to fund their activities, or plan and coordinate physical-world crime (Cross & Shinder, 2008). Based on the nature of an attack, politically motivated attacks can be further subdivided as: protests against political actions, protests against laws or public documents, and outrage against acts related to physical violence (Gandhi et al., 2011).

Economic situations and personal or corporate financial greed often provide motives for cyberattacks. Cyber mercenaries and organized cartels also operate in cyberspace. Other examples of economically motivated attacks include espionage, ransomware, identity theft, piracy, electronic fraud and tax evasion, money laundering, etc. With the growing use of technology, now a new term has emerged, Crime as a Service, and it has already been ranked in the top IT security threats for 2018. Crime-as-a-Service is when a professional criminal or group of criminals develop advanced tools, which are offered up for sale or rent to other criminals or criminal-wannabes who are usually less experienced. Typically, the exchange would occur on the Darknet and it will be through some type of cryptocurrency such as Bitcoin because it is anonymous and essentially untraceable.

Socio-cultural conflict can be viewed as competition between individuals or groups over incompatible goals, scarce resources, or power, including the denial of control to others (Avruch, 2009). Cross-cultural conflict can also manifest as ethnic conflict. Cyber conflicts incited for cultural reasons include conflicts between Taiwan-China (August 1999), Russia-Estonia (2007) and Russia-Georgia (2008). Similarly, the Israel-Palestine cyberconflict, where national symbols – the Israeli flag, Hebrew text, and a recording of the Israeli national anthem – were put into Hezbollah home page (Karatzogianni, 2008), belongs in this category. Gandhi et al. (2011) point out the sometimes the hackers' motivation can also be ethical and that many cyberattacks are motivated by deeply rooted socio-cultural issues.

ROUTINE ACTIVITY THEORY

While cybercrime and cyberterrorism have become problems of growing importance to our society, little work has been done to address the problem from a theoretical perspective and propose an approach grounded in theory. Overall, very few criminological theories have been applied to crimes in cyberspace. Prior work has been focused on explaining contributing factors to malware victimization (Lévesque et al., 2017), the differences and similarities between physical and cybercrimes (Llinares, 2015), as well as understanding privacy attitudes and safety behaviors online. While these studies add knowledge to this growing field of concern, they are predominantly concerned with attacks against individuals and do not explicitly address critical infrastructure. Cyberterrorism is an inherently difficult to explore due to the sensitive nature of the data and the limited opportunities to collect and analyze it. In addition, the gap in research can be explained by the fact that cyberterrorism is a relatively new concept and there is generally a lack of theoretical frameworks to explain it.

The current study utilizes Routine Activity Theory (RAT) to explain cyberattacks against critical infrastructures and SCADA systems. Others have already used this theory when looking into cybercrimes. For instance, Choo (2011) focused on RAT to mitigate risks and opportunities for cybercrimes to occur through making cybercrime more difficult to commit and by increasing the risks of detection and punishment associated with committing cybercrimes. This paper provides an overview of different types of cybercrimes and proposes mechanisms to prevent them. However, the authors do not go into much depth on the issue of cyberterrorism and how RAT can be used to prevent it.

Clarke and Felson (1993) proposed that a crime occurs when there is a likely offender, a suitable target, and a capable guardian is absent (Figure 1). Routine Activity Theory (RAT) has been developed originally to explain physical crime, but it can be also applied to cyberspace.

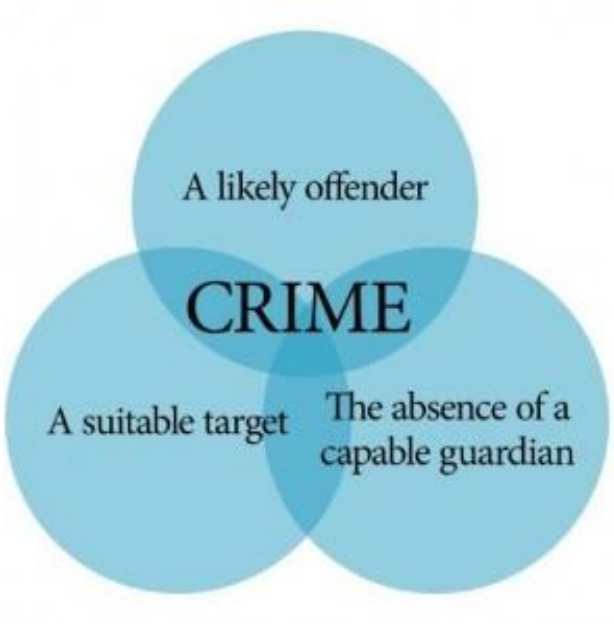

Figure 1. Routine Activity Theory

In a cyberterrorism context, the likely offender would be any of the nation-states such as China, Russia or North Korea who have the capability to launch APT attacks. A suitable target would be any critical infrastructure like a power grid, a dam, a nuclear facility, etc. Those are any type of facilities of importance to national security that require additional security and have extra layers of protection due to their impact on society. And finally, the absence of a capable guardian would be considered the outdated legacy systems and cleartext protocols used for SCADA systems to communicate between the different components.

RESEARCH QUESTIONS

There is a pressing need to address the problem of cybercrime and cyberterrorism. The first step is to focus on the root cause of the problem by developing a taxonomy that can classify existing knowledge on the various types of attacks against critical infrastructure and the motivation of the hackers who launch them. Furthermore, utilizing Routine Activity Theory would be instrumental in taking a rigorous scholarly approach to the topic. This is a novel way of approaching the problem and can assist in the development of more adequate and relevant policies to prevent such attacks in the future. The current study aims to address the following research questions:

RQ1: Can we classify knowledge on cyberattacks against critical infrastructure?

RQ2: Can we utilize Routine Activity Theory to mitigate cyberattacks against critical infrastructure?

The current study is the first attempt not only to create but empirically validate a taxonomy of cyberattacks against critical infrastructure. Thus, we are taking a qualitative study approach and relying on grounded theory to identify themes and to evaluate the proposed classification of knowledge in the field. The goal is to assist practitioners and scholars in improving the guardianship of such facilities of national security and improve the existing incident detection and response practices. This is a crucial step to strengthen the overall security posture of our country.

TAXONOMY DEVELOPMENT

Prior studies have attempted to classify knowledge on cyberattacks against critical infrastructure. Alcaraz and Zeadally (2015) provided a detailed list of security controls derived from a number of US and international standards and best practices. However, the focus of the project was to highlight which controls are most referenced across the standards and derive an inventory of those top controls to prevent cyberattacks against SCADA systems. Another study proposed by Papp et al. (2015) used the Common Vulnerabilities and Exposures (CVE) database to identify five types of cyberattacks: (1) precondition, (2) vulnerability, (3) target, (4) attack method, and (5) effect of the attack. However, these classifications are general and not relevant directly to SCADA systems and critical infrastructure. And finally, (Humayoun, 2011) conceptualize cyber-physical systems (CPS) from a security perspective. They propose a three-dimensional taxonomy that explains cybercrimes based on CPS systems, CPS components, and a security dimension. While others have investigated this issue in the past, the proposed classifications have not been empirically tested due to the sensitive nature of the context.

The current study addresses these gaps and offers a comprehensive classification of cyberterrorism attacks with consideration of the hackers' motivation. With regards to policy recommendations, our focus is on the guardianship aspect of RAT and how the government can better protect the legacy SCADA systems and improve the security posture of these facilities.

The first dimension, hacker motivation, is related to the offenders which could be politically, socio-culturally, and/or economically motivated. The second dimension represents the cyber, physical, and cyber-physical components of any cyber-physical system (CPS) and is a differentiation of the various aspects of the suitable target. The third dimension, security, is related to the threats, vulnerabilities, and controls that represent the lack of the capable guardian. These different dimensions are conceptualized and depicted in Figure 2.

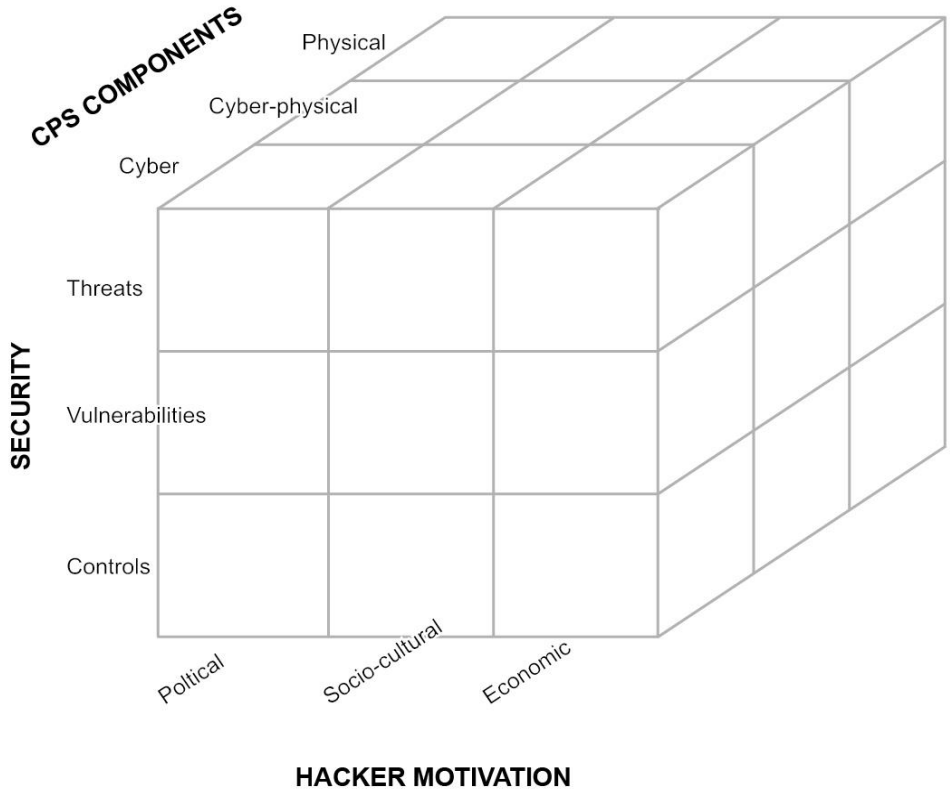

Figure 2. Proposed Taxonomy

METHODOLOGY

The current study utilizes Design Science Research (DSR) methods. This approach is appropriate because it addresses real-world problems of cyberattacks against critical infrastructure through an academic lens and provides a solution that is grounded in research (Hevner & Chatterjee, 2010; Hevner et al., 2004). More specifically, DSR has three cycles, and they are addressed as follows:

- Rigor cycle – an extensive literature review was completed to inform the initial design of the taxonomy.
- Relevance cycle – requirements were derived from the gap in knowledge, skills, and technology that currently exists in the critical infrastructure facilities and the information security professionals who maintain them.
- Design cycle – the taxonomy was initially created based on analyzing academic work, but it was validated and refined through simulations and then we will conduct qualitative interviews with practitioners in the field who are the target of the proposed tool.

To evaluate the taxonomy, we used three scenarios that are based on real-world cyberattacks. These scenarios are informed from publicly available data on prior attacks such as Stuxnet, the Ukrainian power grid shut down, and numerous ransomware attacks against public institutions in the US. The purpose of initially testing the taxonomy with simulations is to evaluate it and document the lessons learned or suggestions for improvement before taking the next step and evaluating it through interviews with practitioners in the field. The themes that emerge from testing the taxonomy with the scenarios can be used to inform the development of empirical generalizations and, in turn, theory to explain cyberattacks against critical infrastructure facilities. The results can help refine the proposed taxonomy and evaluate its utility and usability for practitioners in the field who encounter various cyberattacks and do not have adequate mechanisms to provide effective and efficient guardianship.

The sensitive nature of this project presents a significant challenge to identifying participants and collecting the data. Thus, we created simulations based on publicly available data on cyberterrorist attacks. While the current study predominantly explores the problem from a US-centered perspective, cybercrimes and cyberterrorism are global issues and our methodological approach can be replicated in other countries.

To operationalize the proposed taxonomy, the first step is to explore and explain scenarios that are based on real-world cyberattacks against critical infrastructure facilities. That way can avoid any issues with obtaining access to sensitive top-secret government information. The second part of this project includes conducting a pilot test with several college level students with basic understanding of the topic. They are presented with the taxonomy and the three scenarios and are asked to classify the attacks. This will help to understand whether the taxonomy is easy to use and understand and whether it provides exhaustive information on each of the dimensions.

RESULTS

Scenarios

While we are yet to see a true large warfare effort on a global scale, there have been numerous instances when critical infrastructure and industrial control systems (ICS) have been attacked. Figure 3 shows the history of these attacks over the last two decades and identifies some of the main actors on the global arena that have the potential to cause devastating damages. Some of these countries are USA, Russia, China, North Korea, Israel, and Ukraine. Even though it is very difficult to prove with certainty that an attack was funded by a particular state, there is some information about state-funded cyberarmies such as the ones in China (Hvistendahl, 2010) and North Korea (Haggard & Lindsay, 2015).

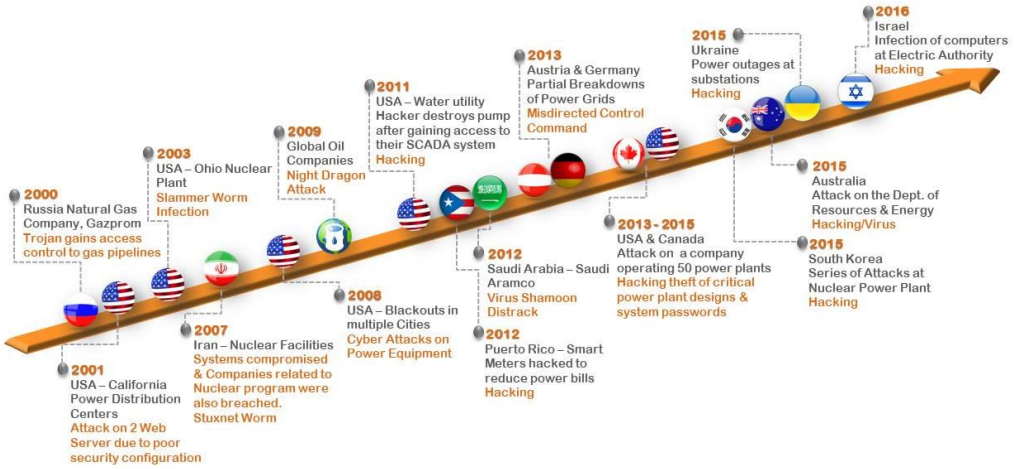

Figure 3. History of Cyberattacks Globally in ICS – adopted from Azarcon (2017)

For the purposes of this study, we used three scenarios to illustrate possible types of cyberattacks against critical infrastructure. Those were informed based on publicly available data on Stuxnet virus, the Ukrainian power grid shutdown, and the numerous ransomware attacks against government facilities in the US. First, we present the scenario, then we test to see whether our taxonomy can effectively explain it, and then we examine possible controls to increase the guardianship aspect of the RAT used to inform the taxonomy development.

Stuxnet

When it comes to cyberterrorist attacks, a real massive cyberwar on a global scale is yet to happen. However, this does not mean that it will not happen one day. Stuxnet opened the door to this type of crime. The purpose of the Stuxnet worm was to sabotage Iran's uranium enrichment program, not spread terror. But the cyberweapon's demonstration effect was enormous, showing the world how cyberterrorism could potentially cause substantial physical damage to critical infrastructures by attacking the computer controllers and SCADA systems that regulate industrial machinery.

The Stuxnet code has spread to computer programmers and hackers around the world. However, its sole victim was the electrical motors and industrial controllers used at Natanz and it did not cause any known damages to other devices (Farwell & Rohozinski, 2011). Almost a decade later, it is still unclear whether non-state hackers have the capacity and the willingness to modify and learn from the code in Stuxnet and other cyber-weapons developed by states to attack other SCADA systems in similar ways. Such uncertainty is troublesome and as Kenney (2015) suggests, "policymakers and computer security professionals should devote greater resources to understanding the potential for non-state actors to exploit cyber-weapons developed by states and how to stymie the spread of this malicious code" (p. 127).

Based on this information, we can classify Stuxnet as follows:

- CPS components: cyber-physical
- Hacker motivation: political and economic
- Security: Threats (external, man-made), vulnerabilities (technical), and controls (vulnerability scanning, penetration testing, log monitoring, and auditing).

What this shows is that Stuxnet is a complex type of cyberattack against critical infrastructure and it can target more than one of the proposed dimensions in the taxonomy. We were expecting this because most SCADA cyberattacks are quite sophisticated and attackers rarely have a single reason to breach such systems.

The value of the taxonomy comes from the fact that based on the attacker motivation per RAT, we can tailor our controls and provide more efficient means of guardianship of our critical assets such as developing plans for identifying and responding to incidents related to national security infrastructure. Being able to detect cyberattacks and respond to them in a comprehensive and timely fashion is crucial for any entity.

Ukrainian Power Grid Shut Down

In December 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers that were due to a third party's illegal entry into the company's computer and SCADA systems. Over 225,000 customers in various areas were affected by the power loss and the Ukrainian government officials claimed the outages were caused by a cyberattack, and that the Russian security services were responsible for the incidents (Lee et al., 2016)

In terms of capability, the attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the IT networks of the electricity companies (Lee et al., 2016). They showed the capability to gain a foothold and harvest credentials and information to gain access to the ICS network.

Additionally, the attackers proved expertise, not only in network connected infrastructure, such as Uninterruptable Power Supplies (UPSs), but also in operating the ICSs through supervisory control system, such as the Human Machine Interface. The SANS report (Lee et al., 2016) presents a level of sophistication of a cyberattack that only a state-funded entity would possess and it also presents some recommendations for critical infrastructure facilities when it comes to cyberterrorism defense.

Based on this information, we can classify the Ukrainian power grid shut down as follows:

- CPS components: physical
- Hacker motivation: political
- Security: Threats (external, man-made), vulnerabilities (technical), and controls (vulnerability scanning, penetration testing, log monitoring, and auditing).

Similar to the Stuxnet virus, the attack against the Ukrainian power grid demonstrates the motivation of nation-state actors to establish power and dominance over other countries and showcase their ability to control critical infrastructure systems. This perfectly exemplifies the need to provide more rigorous guardianship and controls to prevent other attacks like that in the future.

Ransomware Attacks

And finally, our third scenario is based on the numerous ransomware attacks that have been on the rise in the last few years. Some examples include WannaCry and Ryuk. WannaCry is a ransomware worm that spread rapidly through several computer networks in May of 2017. After infecting Windows computers, it encrypts files on the hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

A number of factors made the initial spread of WannaCry particularly significant: it struck a number of important and high-profile systems, including many in Britain's National Health Service; it exploited a Windows vulnerability that was suspected to have been first discovered by the NSA; and it was linked to the Lazarus Group, a cybercrime organization that may be connected to the North Korean government (Fruhlinger, 2018).

Another type of ransomware attack attributed to the same Lazarus Group in North Korea is Ryuk. Unlike the common ransomware, systematically distributed via massive spam campaigns and exploit kits, Ryuk is used exclusively for tailored attacks. In fact, its encryption scheme is intentionally built for small-scale operations, such that only crucial assets and resources are infected in each targeted network with its infection and distribution carried out manually by the attackers.

This, of course, means extensive network mapping, hacking and credential collection is required and takes place prior to each operation. Its alleged attribution to Lazarus Group may imply that the attackers are already well experienced in the targeted attacks domain, as seen by attacks such as the breach of Sony Pictures in 2014 (Cohen & Herzog, 2018).

Some recent victims of such ransomware attacks are the City of Baltimore, Jackson County, and the Atlanta airport. It is interesting to note that Jackson County was one of the few who decided to pay the cyberterrorists and as a result, they paid almost $500,000 in bitcoin to get their data back. These few examples clearly demonstrate the need to develop more rigorous tools for protecting critical assets.

With respect to our proposed taxonomy, such ransomware attacks against SCADA systems can be classified as:

- CPS components: cyber
- Hacker motivation: economic
- Security: Threats (external, man-made), vulnerabilities (technical), and controls (data backup and recovery).

Going back to the two research questions posed in the beginning of the paper, through exploring the three scenarios we demonstrated that the proposed taxonomy can successfully classify knowledge on cyberattacks against critical infrastructure, because the dimensions it is comprised of are broad enough to capture various threats, targets, and security controls. And with regards to the second research question, we established that RAT can, and is in fact, a valuable tool to build our theoretical foundation. It gives us a solid research background that we can use to solve real-world problems such as incident detection and response as prescribed by DSR.

LIMITATIONS AND FUTURE RESEARCH

This is among the first studies of its kind and, as such, it comes with certain limitations. For example, due to the sensitive nature of critical infrastructure facilities, we are severely limited when it comes to collecting data on cyberattacks. Thus, we had to rely on publicly available secondary data. However, our future plans include validating the proposed taxonomy through interviews with information security professionals. That will help us refine and improve our work, following DSR best practices. We encourage our colleagues to further explore the tool we proposed and conduct qualitative interviews with critical infrastructure experts around the world. The scenarios utilized for this study are useful but getting feedback from practitioners is a logical next stage of this project.

CONCLUSION

Cybercrime and cyberterrorism are issues of growing concern, yet not much has been done to address the problem and provide mechanisms for more adequate incident identification and response. We witness cyberattacks every day and if we have credit cards or have shopped in some of the most popular chains, we have already been victims of these attacks. They are especially threatening when it comes to critical infrastructure and national security. Thus, as a society we need to put more pressure on policy makers to address these concerns and provide more effective and adequate regulations to reduce cybercrime and respond to incidents. If as a nation we demonstrate that we do not tolerate these types of crimes, it will send a clear sign to hackers and any individuals with malicious intents that there are severe consequences to their actions. We can start this process by leveraging the Routine Activity Theory and focusing on strengthening our security posture as individuals, corporations, and nation.

The taxonomy we propose in this study is a good first step in addressing this important issue and providing researchers and practitioners with the tools necessary to better understand the challenging environment of cyberterrorism and cybercrime. While there may be many hurdles to proactively addressing the problem such as lack of adequate policies, regulations, resources to investigate these attacks, multiple jurisdictions, and complicated extradition policies, it is our duty to provide better guardianship of critical infrastructure facilities and ensure that we have implemented all the necessary controls to reduce cybercrime and cyberterrorism and that if these crimes were to happen, we will be ready to respond to them.

REFERENCES

Aaronson, L. (2005). For love of money-malicious hacking takes an ominous turn. *Ieee Spectrum*, *42*(11), 17-19.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53-66.

Avruch, K. (2009). Cross-cultural conflict. *Conflict Resolution*, *1*, 45-57.

Azarcon, J. (2017). *Cyber Immunity, a holistic view for Industrial Control Systems*. Retrieved from: https://is5com.com/uncategorized/nov-22-2017-cyber-immunity-a-holistic-view-for-industrial-control-systems/

Beveren, J. V. (2001). A conceptual model of hacker development and motivations. *Journal of E-business*, *1*(2), 1-9.

Choo, K.-K. R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers & Security*, *30*(8), 719-731.

Clarke, R. V. G., & Felson, M. (1993). *Routine Activity and Rational Choice* (Vol. 5). Transaction Publishers. Piscataway, NJ.

Cohen, I., & Herzog, B. (2018). *Ryuk Ransomware: A Targeted Campaign Break-Down*. Retrieved from: https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/

Cross, M., & Shinder, D. L. (2008). *Scene of the Cybercrime*. Elsevier. Amsterdam, The Netherlands

Embar-Seddon, A. (2002). Cyberterrorism: Are we under siege? *American Behavioral Scientist*, *45*(6), 1033-1043.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers & Security*, *18*(1), 28-34.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28-38.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony Hack: Exporting Instability through Cyberspace.

Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22). Springer. New York City, NY.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*(2), 175-186.

Humayoun, S. R., Dubinsky, Y., & Catarci, T. . (2011). A three-fold integration framework to incorporate user–centered design into agile software development. *Human Centered Design*, 55-64.

Hvistendahl, M. (2010). China's hacker army. *Foreign Policy*.

Karatzogianni, A. (2008). *Cyber-conflict and global politics*. Routledge. Abingdon, Oxfordshire

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

Krone, T. (2005). High tech crime brief. *Australian Institute of Criminology, Canberra, Australia*.

Lee, R. M., Assante, M. J., & Conway, T. S. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Retrieved from: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lévesque, F. L., Fernandez, J. M., & Batchelder, D. (2017). Age and gender as independent risk factors for malware victimisation. Proceedings of the 31st British Computer Society Human Computer Interaction Conference

Llinares, F. M. (2015). That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime. In *Cybercrime Risks and Responses* (pp. 47-63). Springer. New York City, NY.

National Research Council. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press, Washngton, D.C.

Nations, U. (1995). The united Nations manual on the prevention and control of computer related crime. *International Review of Criminal Policy*, 43-44.

Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 13th Annual Conference on Privacy, Security and Trust (PST). July 21-23, 2015. Izmir, Turkey.

Poremba, S. M. (2011). Cyber terrorist threats loom 10 years after 9/11. Retrieved from http://www.nbcnews.com/id/44415109/ns/technology_and_science-security/t/cyber-terrorist-threats-loom-years-after/

Quigley, M. (2007). *Encyclopedia of information ethics and security*. IGI Global. Hershey, PA.

Rid, T. (2013). Cyberwar and peace: Hacking can reduce real-world violence. *Foreign Affairs*, *92*(6), 77-87.

Rogers, M. (1999). Psychology of computer criminals. Annual Computer Security Institute Conference, St. Louis, MO.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16-19.

Verton, D., & Brownlow, J. (2003). *Black ice: The invisible threat of cyber-terrorism*. Osborne. London, UK.

Zeviar-Geese, G. (1997). The State of the Law on Cyberjursidiction and Cybercrime on the Internet. *California Pacific School of Law, Gonzaga Journal of International Law*, *1*, 119.