Winter 2-1-2020

Increasing Connectivity Means Increasing Civilian Vulnerability in Developed and Developing Countries

Yara Amelia Contijoch

Increasing Connectivity Means Increasing Civilian Vulnerability in Developed and Developing Countries

Yara Contijoch

Fordham University

Fordham College at Lincoln Center

International Studies Thesis

Fall 2019

Abstract

Although interconnected devices and networks have expanded the possibilities of what was previously thought possible across numerous fields, it has also led to increased civilian vulnerability through cyber-attacks. This project investigates civilians' vulnerabilities through four cyber-attacks: (1) the Anthem health insurer cyber-attack in the United States, (2) WannaCry ransomware on the National Health Service in the United Kingdom, (3) the Jasmine Revolution cyber-attacks in Tunisia, and (4) the 2010 Natanz uranium enrichment facility cyber-attacks in Iran. These four case studies depict that regardless of civilian prosperity, perceived national security, and geographic location, civilians are increasingly vulnerable to attack due to increased interconnectivity. Their vulnerability and the victimization that follows is analyzed according to Spini's Vulnerability Framework, which is used to investigate the resources, stressors, outcomes, and contexts of civilians throughout their respective attacks. Upon demonstrating these vulnerabilities, this project concludes with suggestions for further research and means to reduce civilian vulnerability and victimization moving forward.

Table of Contents

Introduction

For hundreds of years, a state's military and geography were significant in determining the state's and its civilians' security. Today, however, this is an argument growing increasingly inapt as states turn to cyber-warfare. When the computer was first invented, its creators did not expect the device to impact and dictate every aspect of our lives, from national infrastructure to heart monitors to doorbells. Because of technology, our lives are exploding with opportunities. Few, however, are aware of the costs. Interconnected devices, whether they be computer labs or nanny cams, are connected to networks and by these means, information can move. We can send emails and videos and access websites around the world, but this same information can be stolen remotely as well. For those nearby, these devices and networks make it even easier to steal or attack anything digitized or connected to a network. In developed countries, we hear about election interference and stolen credit card numbers and email accounts, but this is only the tip of the iceberg. Interconnectivity, while certainly beneficial, opens users to vulnerabilities, from which they were previously protected. A state's military and geography, even one's personal prosperity and security efforts, are no longer enough to protect individuals as they become increasingly reliant on interconnected devices. By these means, warfare is changing, leaving individuals increasingly vulnerable and susceptible to attack.

With the development of cyber-space, the goals and capabilities of attackers are evolving, increasing the range of potential victims. Scholars suggest that the major concern in security "is no longer weapons of mass destruction, but weapons of mass disruption" (Akarcay and Ak, 197). For example, one goal of cyber-warfare revolves around "the economic interests of the predator to preserve and exploit, rather than attack and destroy the target economy and its cyber infrastructure" (Akarcay and Ak, 198). In exploiting others, attackers can benefit repeatedly, say year after year.

On the other hand, dedicated attackers could also destroy "entire infrastructure…crippling the nation" (Akarcay and Ak). One may even consider how the first of these could also lead to the second over time. Meanwhile, the low cost of these attacks not only drives attackers to use cyber-warfare, but also enables attackers that have been incapable of acting out before. Through cyber-attacks, "non-state actors and small states can play significant roles at low levels of cost" (Akarcay and Ak, 198). Those who "are normally incapable of competing militarily or economically" can more successfully attack their targets and "offset conventional disadvantages" through cyber-attacks (Akarcay and Ak, 200, 205). These enabling factors make it so that state and non-state actors can compete with domestic or international powers they oppose. By these means, traditional notions of security grow increasingly irrelevant and security superpowers and their civilians grow vulnerable.

Distinct from previous military advancements, cyber-attacks also lack the deterrent factor that other weapons have. For example, if one country carries out a kinetic attack on the other, it is likely that the victim will retaliate with another kinetic attack.[1] However, when it comes to cyber-warfare, it can be "difficult and time-consuming to identify an attack's perpetrator," it "may take months, if identification is possible at all" (Gazula, 22). Attackers might even be able to make it look like it was sent from somewhere or someone else. With the ability to keep their identities confidential, state and non-state actors can use cyber-attacks without the fear of the target retaliating against them. Taking matters a step further, if a non-state actor is identified as the attacker, "it may have no assets against which the target nation can retaliate" against (Gazula, 22). For these reasons, cyber-attacks are attractive for both small and large state and non-state actors.

[1] Kinetic attacks, warfare, and security refer to the physical versions of these. In other words, when militaries face each other on land, sea, or air. In this project, cyber-attacks, warfare, and security are the opposite in that they are not physical, rather they occur in cyberspace.

The security of interconnected devices, or perhaps the inherent lack thereof, increases the attractiveness of cyber-attacks and the vulnerability of its users even further.

Civilian vulnerability to cyber-attacks is in part due to the vulnerabilities of the technologies themselves. Technological vulnerabilities refer to vulnerabilities in the networks, hardware, software, and due to the user. With regard to vulnerabilities in networks, one must note that in cyberspace the offense has the upper hand (Gazula, 22). For example, the Internet was designed "to be collaborative and rapidly expandable and to have low barriers to technological innovation" which made "security and identity management…lower priorities" (Gazula, 22). With security and identity management as low priorities, perpetrators have the upper hand on the offensive as they constantly search for ways to bypass security efforts. In such an "offense-dominant environment", "a fortress mentality" for one's software and hardware with hardcoded defenses "will not work" (Gazula, 22). Instead, "the strongest and most elaborate defenses are turned into a cumbersome liability and a disadvantage" that may not be able adapt to a particular need during an attack (Akarcay and Ak, 197). Overall, this structure suggests a usability-security seesaw, meaning that the more secure a device or service may seem, the more cumbersome it can be for both the user and the security team. On the other hand, technology that is very fluid and user-friendly, like the Internet, may result in lower security if the proper defenses are not in place to adapt to the attack. Engineers and security specialists must then determine where to strike the balance between usability and security.

In addition to this tradeoff that affects networks, hardware, and software, the cost of these devices and services can result in technological vulnerabilities as well. Many devices and services "are currently manufactured for low cost and speed, often resulting in few cybersecurity features" (Tschider, 120). Most devices that do have security features do not include regular updates, so

when vulnerabilities are found they are left unpatched and vulnerable to attack (Tschider, 120). In a similar fashion, manufacturers are creating devices and services without the assistance of technology companies, leaving these products and their consumers without any protections whatsoever (Tschider, 117). Finally, as secure as some manufacturers and administrators might make their networks, hardware, and software, there is always the possibility for human error via social engineering attacks.[2] These factors depict some of the technological vulnerabilities that can be exploited for cyber-attacks on civilians.

The ways in which civilians use technology depict the ways in which they are vulnerable as well. In developed countries, our use of technology is so expansive that it knows "how we work, play, shop, sleep, drive, manage our homes, and medicate" (Gorman, 1). Developed countries use devices that monitor babies; remind individuals to take their medicine or dispenses it for them; record activity and sleep; remotely monitor homes and appliances; and monitor traffic, pollution, energy usage, the structural soundness of buildings, etc. (Gorman, 2). There are also "electronic airport, civil, and military air traffic and air space control systems"; electronic systems that design and develop hardware and software used in civilian and military aircrafts; "electronic national defense systems, fully-automated subway control systems, water supply and control systems, hospital electronic systems, electronic emergency management systems, electricity grid management systems, railway electronic systems, financial and banking systems"; and more (Akarcay and Ak, 201). These technologies in developed countries can be targeted at any time to victimize civilians individually or as a society. This project will look at two case studies depicting the two types of cyber-attacks, passive and active, that have occurred in developed states on some

[2] Social engineering attacks trick users into disclosing sensitive information, such as usernames, passwords, or credit card details. Unlike hacking, social engineering relies more on trickery and psychological manipulation than technical knowledge.

of these systems. The first of these will be the Anthem health insurance cyber-attack in the United States and the second will be WannaCry ransomware attack on the National Health Service in the United Kingdom. Through these cyber-attacks, this project demonstrates civilian vulnerability and victimization as a result of growing interconnectivity in developed countries.

In developing countries, technology is used both personally and in society, but often to less of an extent than in developed countries. Throughout the Middle East, Africa, and Asia many individuals have smart phones that are critical to their lives (GSMA, 3). In some contexts, technology is also used to better offer humanitarian assistance. This includes "distance learning via the Internet"; increased connectivity brought by giants like Facebook; 3D printers to "manufacture prosthetic limbs"; "solar lighting in dozens of camps and solar-powered water pumps"; and more (Aleinikoff, 547). Technology, especially in the form of mobile phones, enables individuals "to find employment, run small businesses and work in ancillary services, such as selling charging or credit services and mobile phone repair, as well as mobile money services" (GSMA, 4). Naturally, their phones are also critical to help them stay in touch with family and friends and ensure family reunification when they have been separated (GSMA, 4). Humanitarians and innovators continue to explore how technology can improve lives further for those in developing countries and regions. Many anticipate that future efforts may involve additional banking and employment efforts as well as improved disaster management (Talukder and Patnaik). These uses of technology can translate into an array of vulnerabilities for civilians.

To depict some of these vulnerabilities, this project will also include two case studies depicting passive and active cyber-attacks in developing countries. One of these will be the Jasmine Revolution cyber-attacks in Tunisia and the 2010 Natanz uranium enrichment facility cyber-attack in Iran. Although this second attack occurred on what is suspected to be a national

plant, its analysis will explore how a similar attack could be conducted on a civilian power plant. By these means, this project will depict civilian vulnerability due to interconnectivity in developing countries, in addition to the aforementioned similar vulnerability in developed countries.

Overall, this project explores how civilian vulnerability is increasing as a result of evolving and increasing interconnectivity. This relationship has no regard for civilian prosperity, perceived national security, or geographic location, despite these factors being significant in protecting against kinetic attacks. Instead, interconnectivity enables attackers around the world to target a wider range of potential victims. The low cost and anonymity of cyber-attacks further enables these attackers. Because government borders and militaries do not necessarily protect civilians from cyber-attacks, they are at risk in a relatively new way. This project intends to investigate their vulnerabilities and how their vulnerability worsens when victimized by cyber-attacks. I find that traditional safeguards have been ineffective in protecting civilians from cyber-attacks and so, civilians in developed and developing countries are equally susceptible to attack, regardless of prosperity, perceived national security, and geographic location.

This project provides a thorough investigation of this equal susceptibility to cyber-attacks. First, I will present my methodology, explaining my case selection and introducing Dario Spini's Vulnerability Framework, which I use to demonstrate and investigate civilians' vulnerabilities and victimization throughout the four case studies. Second, I examine the limitations of this project and how I address them. Next, I review the literature that includes an interdisciplinary range of scholarship in the fields of cybersecurity, humanitarian studies, and political science, examining how they intersect when exploring civilian vulnerability to cyber-attacks. Then, I provide a more thorough explanation of the theoretical framework before turning to the case studies, analyzing

how each attack affected civilians in terms of vulnerability and victimization. I will conclude with questions for further research and options for managing civilian vulnerabilities.

Methodology

This project investigates the fields of cybersecurity, humanitarian studies, and political science to explore increased civilian vulnerability due to interconnectivity in both developed and developing countries. Most of the sources used are academic journals from the fields of cybersecurity, humanitarian studies, and political science found through the Fordham University database and other international scholarly databases. Other sources include online news articles, interviews, and press releases for specific details of events regarding cyber-attacks in both regions.

By studying cyber-attacks in developed and developing countries, this project demonstrates that civilians are increasingly vulnerable regardless of their prosperity, perceived national security, and geographic location. This project specifically looks at attacks in the United States, the United Kingdom, Tunisia, and Iran, where the first two are categorized as developed countries and the last two are categorized as developing countries. This distinction is made to represent the difference in lifestyle for civilians in these countries. In this project, the United States and United Kingdom are categorized as developed, due to the prosperity of their civilians and the strength of their security agencies relative to Tunisia and Iran. Tunisia, meanwhile, is considered a developing country in this project, because of the economic instability and theories of lingering corruption from the previous dictator, Zine el-Abidine Ben Ali. Iran is also considered a developing country due to corruption, misuse of resources, and discrimination against women and ethnic and religious groups. These categorizations are consistent with the United Nations' World Economic Situation and Prospects 2019 categorization of developed and developing countries. For

this project, this distinction serves to demonstrate the different contexts of attacks on civilians, regarding civilian prosperity and perceived national security, in each of these countries.

These countries were also chosen to demonstrate how geographic location does not reduce one's vulnerability to cyber-attacks. Whereas with kinetic warfare, proximity and state borders have significant roles regarding offense and defense, this is not the case with cyber-attacks. Anyone, including civilians, can be targeted from anywhere in the world through computer networks, regardless of how far away they may physically be. To demonstrate this, this project looks at countries in North America, Europe, and the Middle East and North Africa. It is worth noting that I considered investigating cyber-attacks in South America. However, I chose to investigate the cyber-attacks on Tunisia and Iran, rather than recent cyber-attacks on Mexico, Brazil, and Chile, because these attacks, which were all on banks, closely resembled the cyber-attack on the United States' insurance company, Anthem, in how civilians' confidential information was compromised. Meanwhile, the Tunisian and Iranian attacks were more distinct, which allows this project to demonstrate a wider range of civilian vulnerability and victimization. Similarly, in Asia, Indonesia and Singapore have had their hospitals and healthcare systems attacked, so this project aims to demonstrate the similarity of their civilian vulnerability through the attacks on the United Kingdom National Health Service. Finally, in Africa, mobile phones are growing increasingly common and computer systems and data centers are being used for education and other methods of infrastructure, like Tunisia and Iran, and therefore, have similar vulnerabilities as well. Although this project does not intend to generalize regions of the world, this project investigates these cyber-attacks to demonstrate a few varied geographic locations and civilian vulnerabilities.

These attacks in the United States, the United Kingdom, Tunisia, and Iran are explored as four individual case studies with each one demonstrating not only different contexts for civilian life, but also different types of attack. After dividing the case studies according to relative civilian prosperity and perceived national security, these case studies are then divided further based on the type of attack, passive versus active attack. Passive attacks are those that collect information, while active attacks manipulate information and likely have a secondary purpose that influences the real world. This project looks at both types of attacks in opposing contexts to demonstrate civilian vulnerability regardless of civilian prosperity, perceived national security, and geographic location. Accordingly, the attacks on the United States and Tunisia are the studied passive attacks, while the attacks in the United Kingdom and Iran are the studied active attacks.

To explore civilian vulnerability and victimization, this project will use Dario Spini's Vulnerability Framework which analyzes civilian resources, stressors, outcomes, and contexts. In conducting the analysis, this project uses tables to clearly organize the assessment of these four factors throughout each cyber-attack. By these means, this project demonstrates that interconnectivity results in growing civilian vulnerability and victimization without regard for civilian prosperity, perceived national security, and geographic location; factors that historically protected civilians.

Limitations

This project faces a few limitations. The first of these is that the great majority of sources regarding cybersecurity focus on the technical component of cybersecurity rather than the human element. For example, they may analyze the technical vulnerability in a program's code. Very few sources focus on the human component, meaning how those victimized by a cyber-attack are

affected by the attack, both during and afterward. I see this matter as a grey area between computer science and the social sciences. Research on this topic, however, does not yet seem to be a major focus in the social sciences as demonstrated by the lack of sources available on international scholarly databases. Some sources indicate the vulnerability of certain systems and programs, like medical devices and internet communities, but few, if any address how this personally affects civilians. I was only able to find one source where two quotes from individuals affected by a cyber-attack expressed their frustration. It was a journal article written by Rachel Clarke and Taryn Youngstein regarding the WannaCry ransomware attack on the United Kingdom's National Health Service (Clarke and Youngstein, 410). Other than this one source, few, if any, focus on how civilians feel during and after a cyber-attack. Do they feel susceptible to further attack? In addition to frustration, are they sad, scared, or surprised? Do they feel as though this was inevitable? Do they feel indifferent? These are questions that have yet to be explored in computer science or the social sciences. By understanding how certain attacks cite certain emotions, this may indicate what makes civilians feel most harmed and affected. Identifying the attacks that do this may help to identify the attack surfaces that are most vulnerable and need the most protection.[3] As is, these investigations have not yet been conducted, so this project attempts to identify a variety of today's vulnerabilities.

Another limitation is the lack of reports regarding cyber-attacks in developing countries, which may occur for a variety of reasons. One possibility is that the reports exist, but in the language of where the attack occurred, and so I could not access them. Another possibility is that the reports might not be publicized. Another possibility is that the reports might document technical difficulties, but the victims might not realize it was a cyber-attack and so it does not get

[3] Attack surfaces are the reachable and exploitable vulnerabilities in a computer system that may be attacked.

attention as such. Yet another possibility is that the institutions might not document technical difficulties or cyber-attacks, because it may seem insignificant to do so to them. One must recognize that cyber-attacks often go unnoticed or are assumed to be normal technical difficulties unless you are highly skilled and looking for irregularities in a system or network. As a result, individuals and institutions are often unaware that they are being attacked. I suspect that there are few reports documenting cyber-attacks in developing countries for these reasons. Due to the low number of available cyber-attack reports in developing countries, I choose to investigate the 2010 Natanz uranium enrichment facility cyber-attack in Iran as the fourth case study of an active attack in a developing country. Although this attack was performed on what is suspected to be a government plant for the use of a nuclear weapons program, this project demonstrates how a similar attack conducted on a civilian power plant in a developing country may affect civilians' vulnerability and victimization.

Similar to the limitation of few cyber-attacks reported in developing countries, there is a lack of sources that investigate the technological vulnerabilities of devices used in developing countries and humanitarian contexts. The use of technology in many such contexts began only recently, so it is possible that this is simply due to their relative youth. Still, there is not as great an abundance of research on technology in developing countries as there is on technology in developed countries. This project navigates this limitation, by examining sources that come from the field of humanitarian studies that demonstrate the ways in which technology is being used in developing communities. By understanding how technology is used, once can deduce potential vulnerabilities.

Finally, the last limitation is the length of this project. In combining cybersecurity, humanitarian studies, and political science, there are many topics that can be explored further

regarding the increased vulnerability of civilians as a result of interconnected goods and cyber warfare. However, due to the amount of time in which this project must be completed, its investigative scope is limited. As such, this project focuses solely on civilian vulnerability due to cyber-attacks in the stated contexts.

Literature Review

Contribution to Scholarship

There is little scholarship on the intersection of cybersecurity, humanitarian studies, and political science. This paper will tie these three topics together to create a cohesive understanding of their relationship in a time where civilians around the world are increasingly reliant on interconnected devices. This incorporation of and reliability on interconnected devices results in increased civilian vulnerability. To explore this, I will first demonstrate how these three fields interact with one another through the use of technology in distinct contexts.

Cybersecurity Sources Explore Technological Vulnerabilities in Developed Countries

The list of interconnected devices in many developed countries is constantly growing and seemingly endless. Those who study and work in cybersecurity focus on how these devices can be taken advantage of. As such, scholarship in the field of cybersecurity focuses primarily on the vulnerabilities of interconnected goods. The literature in this subsection will focus on the vulnerabilities of societal and medical infrastructure in the United States and United Kingdom respectively and how they leave civilians increasingly vulnerable to attacks. These sources were chosen because they demonstrate a multidisciplinary approach rather than a solely technical or social approach, which is crucial to address civilian vulnerability to cyber-attacks.

Pinar Akarcay led the project "Rethinking Cyber Warfare: Timeless, Normless, and Unconstrained". This work is significant to this project, because of its multidisciplinary approach regarding cyber warfare and society, exploring "the question of national security in light of the cyberspace phenomenon" (Akarcay and Ak, 195). Akarcay references the idea that the major concern for national security today "is no longer weapons of mass destruction, but weapons of mass disruption" (Akarcay and Ak, 197). Most cyber-attacks cause mass disruption, but this is especially true for the first case study where 78.8 million civilians had their names, birthdates, social security numbers, home addresses, and potentially their medical information and financial details (i.e., credit card and bank account numbers) stolen in the Anthem cyber-attack in the United States (Matthews). This event raises the question that if an insurance giant like Anthem cannot protect the information of civilians in the United States, is any one's information anywhere safe?

Attacks, like the Anthem cyber-attack, can lead civilians to lacking trust and confidence in organizations and their ability to keep private information safe. Accordingly, Akarcay suggests that the immense reliability developed countries have on interconnected devices can be a weakness. She writes, "Nations with a low level of IT development….retain…a relative strength," because in the event of an attempted counter-attack against them, there would be a limited number of targets and few, if any, would have crippling effects if taken down (Akarcay and Ak, 201). In contrast, a nation where technology is implemented throughout and relied on heavily has an abundance of targets, including civilians unfortunately. As a result, civilians are not wrong to question the ability for their information to remain secure.

Patricia AH Williams led the project "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem" at Edith Cowan University and at the Security Research Institute in Australia. This research group has an international reputation in leading

digital security with a range of investigative studies. In her work, Williams presents how "increased connectivity to existing computer networks has exposed medical devices to cybersecurity vulnerabilities from which they were previously shielded" (Williams, 305). In demonstrating these vulnerabilities, she hopes to raise awareness to address "patient safety concerns," because as is, "patient safety is under threat" (Williams, 305). Williams writes that although interconnectivity has improved lives within and outside of medicine, the vulnerability of medical devices and systems is of increasing importance, because it "will directly affect clinical care and patient safety" (Williams, 305).

This was exactly the case when WannaCry ransomware made its way into the United Kingdom's National Health Service. Although interconnected goods have made providing services more organized, efficient, and expanded what is possible, the numerous vulnerabilities of the National Health Service's systems left it to be one of the first large and significant organizations affected by WannaCry ransomware. Over sixteen hospitals and additional general practices, health groups, and other medical organizations suffered in one way or another throughout the United Kingdom ("Major Ransomware…" ; Clarke and Youngstein).

Williams provides a comprehensive explanation of how technical vulnerabilities develop into these attacks and how these attacks leave civilians as both patients and employees of the health care system vulnerable. Regarding patients, these vulnerabilities include but are not limited to "potentially incorrect clinical decisions" because of altered information, devices being operated by attackers, and critical alerts regarding a patient not being correctly transmitted or received (Williams, 309). Employees and the health care systems themselves are vulnerable when attacks interfere with regulation compliance, cause reputational and financial damage, leave devices non-operational, and more (Williams, 309). Williams goes on assessing these vulnerabilities, and

exploring risk management, regulation, and standards. She finishes by addressing the idea that "patient safety will always come before cybersecurity requirements," but that the medical and cybersecurity communities must constantly work to close this gap (Williams, 309). In other words, she states that medical practices that are beneficial to patients will always be of greater importance than potential cyber-attacks on them. Although it may be a challenge to close this gap with evolving cybersecurity threats and medical practices, Williams hopes the detrimental risk these vulnerabilities pose will lead to the medical community getting the attention it deserves to secure devices and systems to reduce patient vulnerability.

Humanitarian Sources Explore the Use of Technology in Developing Countries

While cybersecurity sources focus on technological vulnerabilities in developed countries, humanitarian sources focus on how technology is used in many developing countries. This difference in scope is inherent to the lenses of the field where these sources are coming from. As previously stated, I look at humanitarian sources that depict the use of technology in developing countries to deduce potential vulnerabilities. I do this because of a lack of sources that explore the vulnerabilities of technology in developing countries. Upon exploring some uses of technology in these contexts, the potential vulnerabilities will be tied to the case studies regarding Tunisia and Iran to explore the vulnerabilities of those who came under attack.

Alexander Aleinikoff is a well-known figure in the international community for working with migrants and refugees. He has held many honorable positions, including the Deputy High Commissioner for the United Nations High Commissioner for Refugees (UNHCR). In his work "The Present, Past, and Future of Refugee Protection and Solutions: Camps, Comprehensive Plans, and Cyber-Communities", Aleinikoff tells a few migrant stories and how governments and the

international community can offer help to these individuals and their communities. Throughout his work, he demonstrates that connectivity can be of great use and assistance.

Individuals in developing countries, migrants and refugees, and others facing humanitarian crises use technology to improve and restore lives. For those on the move, mobile technology is used "to plan travel, check weather reports, communicate with family (and smugglers), and avoid border closures and border police" (Aleinikoff, 547). Aleinikoff also writes about individuals linked online through a variety of social media platforms. These virtual communities serve a variety of purposes: "providing members with news", "creating a space for political discussions", and "maintaining cultural links" if community members have left home or perhaps certain cultural practices have become unwelcome (Aleinikoff, 547). It is clear how beneficial social media and virtual communities can be to many individuals in a variety of contexts, however, a lack of knowledge regarding these programs can endanger the individuals using them.

Although the work of Aleinikoff and many others demonstrate how technology assists those in developing countries and humanitarian crises, these works often lack consideration for the vulnerabilities of such technology. For example, while social media did offer a platform for political discussion and organization in Tunisia, the government also used it to easily locate those who opposed authorities (Gazula, 45-47). One must consider this relationship. Just as scholars explore potential uses of technology, their costs must also be investigated. Taking matters a step further, it is possible that many users would want to be informed of these vulnerabilities if they knew they could be affected in the way the Tunisian public was in the Jasmine Revolution cyber-attacks.

Just as personal devices are used in developing countries, larger computer systems and data centers are used as well. In working with the Jesuit Refugee Service and its Jesuit Commons High

Education at the Margins program (JC: HEM), Petra Dankova served as Assistant Project Director and Coordinator in Kakuma Camp, Kenya. The first of these two programs, the Jesuit Refugee Service, is an international Catholic organization with a mission "to accompany, serve, and advocate the cause of refugees and other forcibly displaced people" (*JRS USA*). Among their efforts, the Jesuit Commons High Education at the Margins program "brings higher education to those…who have limited access to or are underserved by high education" ("Jesuit Commons…"). In working with these programs, Dankova contributed to creating higher education opportunities for refugees in Kakuma Camp, Kenya in 2011. In her piece, "Technology in aid of learning for isolated refugees," Dankova writes about the JC:HEM's effort to provide access to tertiary education in refugee settings by "linking university teachers in the U.S. with students in refugee camps in Kakuma" (Dankova, 11). The lack of resources and the difficulty to provide and maintain these resources in such contexts however, presents a major challenge and ultimately, great vulnerability.

Providing education through digital lessons in refugee camps and developing countries is being piloted and implemented throughout the world with their vulnerability lurking in the shadows. Like in Kakuma, these efforts often involve creating sites with entire computer labs and internet connectivity, which may or may not already exist or be too slow for these new purposes (Dankova, 11). Naturally, this also means "modern computers", "secure buildings", "a constant supply of electricity", and "technical expertise in country" and in a context where resources are already often scare (Dankova, 12). With the high costs to bring in and maintain these standards, the quality of devices and services can suffer in an attempt to keep costs low leading to vulnerability (Tschider, 120). For example, if resources are left insecure to save money, these resources may be digitally or physically sabotaged by those who oppose such education labs (and

the investment would be lost). On top of that, many students often do not have the proficiency of using a computer and the internet (Dankova, 12). This not only poses a challenge for delivering educational services, but it opens these computer systems and data centers up to great vulnerability if a user accidentally enables an attack by downloading a program with malicious code embedded in it or visiting an insecure website.[4] This could, in turn, give an attacker access to the system or network. By these means, larger computer systems and data centers become vulnerable to damaged hardware or software, attackers altering transmitted information, and more.

In the same way that these large computer systems and data centers for educational programs can be vulnerable due to rigorous demands and potential low skill on the user's end, these same vulnerabilities apply to the large systems that run power plants. Through known vulnerabilities in the software that controls the centrifuges at the Natanz uranium enrichment facility in Iran, attackers used a malware that altered the speed at which the centrifuges spun and altered the systems that monitor the plant overall and enable a plant shutdown (Broad).[5] It is unknown whether Iranians lacked the resources to protect the known vulnerabilities or were simply unaware of them. Either way, the great demands of these larger systems and the potential low skill or education of the users led the centrifuges to being attacked and destroyed. Although this was a government plant, one can imagine how an enemy could attack a civilian power plant in a similar way, interrupting and potentially destroying civilian infrastructure.

[4] Code is the language that tells a computer program what to do.
[5] Malware is short for malicious software. Malware refers to programs that intend to damage a system or do some other type of unwanted activity, such as collecting information.

Political Science Sources Explain Specific Attacks and Warfare

Political science is the third subject this project draws upon to contribute to the explanations of cyber-attacks. Political science also helps explain how cyber warfare fits into accepted notions of warfare and how this increases civilian vulnerability. Regarding the relationship between cyber warfare and traditional warfare, this project also briefly looks at how international law interacts with cyberspace and interconnected goods to reveal civilian vulnerability.

First, the work of Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies", is significant to this project for two reasons: he demonstrates how "the data weapon" fits into today's warfare between state, non-state, and local actors and provides case studies of 24 cyber-attacks around the world from 1982 to 2017 (Gazula). Gazula wrote this paper as a part of his Master of Science in Engineering and Management at the Massachusetts Institute of Technology (MIT) and the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, a department within MIT, published it. I chose to include this source in the political science section, because of its focus on conflict analysis. This source, however, is multidisciplinary and offers detail regarding the technical components of cyber warfare as well.

In his work, Gazula first expands on what he refers to as the "data weapon". He writes about how cyber-attacks provide an element of surprise that cannot be achieved by traditional and kinetic weapons (Gazula, 19). For example, when a cyber-attack is conducted, the victim may not realize that they have been targeted until the moment in which the payload is already delivered or the attackers use the already stolen information.[6] This lies in contrast to physical attacks where the victim might see the weapons or attackers headed for the target. Later, Gazula also writes about

[6] The payload is what a program does to a system after being activated, often as a part of a malware. The payload may involve damage or may involve benign but noticeable activity.

how individual, non-state actors have taken to cyber-attacks to generate revenue and for the purpose of identity theft (Gazula, 21). With the ability to download hacking tools off the internet and purchase more complex ones if desired, even individuals with low levels of skill have been able to take advantage of vulnerable systems (Gazula, 21). At the same time, Gazula tells of the ease and affordability of cyber-attacks, which is beneficial not only to individual actors, but also state actors. Gazula quotes Bill Woodcock, a research director at a nonprofit that tracks Internet traffic, who says, "You could fund an entire cyber-warfare campaign for the cost of replacing a tank tread, so you would be foolish not to" (Gazula, 21). Understanding these matters enables one to understand the growing magnitude of cyber-attacks, which can be used to target civilians if desired.

Gazula also provides case studies of 24 cyber-attacks around the world. This source is significant not only in Gazula's assessment of "the data weapon", but also in the sense that this source acted as a springboard to choose case studies for this project due to his detailed explanations and break down of multiple attacks and their contexts.

Building on all these matters, Cameron H. Bell's paper "Cyber Warfare and International Law: The Need for Clarity" demonstrates how current international law lacks the ability to keep up with the advancements of cyberspace and cyber-attacks. In his work, he identifies clear gaps in the relationship between international law and cyber warfare that are supported by legal and military experts. His work is also significant to this project, because he looks at case studies as well. Among his case studies, he explores the cyber-attack on the Natanz uranium enrichment facility in Iran and its role when exploring the relationship between cyber-warfare and international law. Identifying the gaps between international law and cyber warfare demonstrates the lack of protections in place for civilians in the event of cyber-attacks.

In looking at specific United Nations General Assembly Resolutions, Bell identifies how cyber warfare falls through resolutions regarding aggression due to their ambiguity. While previous military advancements adhered to agreed upon norms and agreements, cyber warfare does not. Bell demonstrates how U.N. Resolution 3314: Definition of Aggression is at the root of the problem in numerous ways. Bell argues that while the international system recognizes that the resolution is not exhaustive, its current stance leads many to the conclusion that only physical actions by state actors are considered acts of aggression (Bell, 26). With this, not only do cyber-attacks fall through the regulation, but actions by individual actors as well. By presenting the Iranian Natanz uranium enrichment facility cyber-attack however, Bell demonstrates "that cyber weapons can act in a similar fashion to conventional weapons in their ability to destroy or dismantle infrastructure" (Bell, 32). At the same time, the suspected attackers, the United States and Israel, also violated Iranian sovereignty when they destroyed the centrifuges (Bell, 32). Given this context, Bell argues that this should be considered an act of aggression. However, because the attack occurred in cyberspace, many argue otherwise.

These opposing views contribute to the lack of international communication between state actors regarding the norms and expectations of cyber warfare. As a result, Bell argues that the international community is increasingly unstable with appropriate and proportional expectations unknown, if considered at all (Bell, 23). With regard to the Iranian uranium enrichment facility cyber-attack, Bell writes:

> "…if Iran responded with a conventional attack on Israel, they would have risked being labeled the aggressor in the eyes of the international system, despite simply responding to a damaging attack on their state infrastructure" (33).

Without discussion regarding the expectations of cyber warfare, there will continue to be uncertainty regarding proportionality. The difficulty and sometimes inability to distinguish

between civilian and state networks and systems can also escalate attacks more than intended if an unintended target is victimized. In addition, with state actors held unaccountable, it is likely that individual actors that attack internationally will not face penalties either. With no set boundaries, penalties, or efforts to resolve growing civilian vulnerability, cyber warfare and the victimization of civilians may increasingly worsen.

Theoretical Framework: Spini's Vulnerability Framework

To explore civilian vulnerability, this project uses a vulnerability framework created by Dario Spini, Doris Hanappi, Laura Bernardi, Michel Oris, and Jean-Francois Bickel. The Swiss National Science Foundation, which is funded by the Swiss government, and the Foundation's branch, the National Centres of Competence in Research (NCCR), supported and published their work. The NCCR works to address and resolve pressing problems, not limited to education, technology, and the promotion of women, and works through higher institutions in Switzerland and international networks ("National Centres…"). These researchers hoped to create a framework that could be used across disciplines to explore vulnerability as it "can be understood both as a state and as a process" throughout life (Spini et al., 1). They define vulnerability as:

> "…a lack of resources, which in a specific context, places individuals or groups at a major risk of experiencing (1) negative consequences related to sources of stress; (2) the inability to cope effectively with stressors; and (3) the inability to recover from the stressor or to take advantage of opportunities…" (19).

Their dynamic framework looks at four main concepts to assess this vulnerability: resources, stressors, outcomes, and contexts (Spini et al., 1).

By investigating the resources, stressors, outcomes, and contexts of civilians throughout cyber-attacks as per Spini's Vulnerability Framework, civilian vulnerability and victimization is dynamic and evolving. According to this framework, resources refer to biological, psychological,

and social resources, including coping strategies, social networks, and support systems in this project (Spini et al., 13). The creators of this framework note that previous findings "have shown that the extent to which individuals are able to mobilise appropriate resources is a strong indicator of their vulnerability or risk to experience hazardous or chronic stressful conditions" (Spini et al., 14). Stressors can include major life events that "modify the individual's functioning" or thinking, chronic strain, such as "enduring problems, conflicts, or threats," or "daily hassles" that are "relatively minor events" (Spini et al., 14-15). "Non-events", or "the absence of expected events," may also be stressors, such as not being in school or employed as expected (Spini et al., 15). In this project, the cyber-attacks themselves can be considered stressors in addition to other stressors in civilians' lives. Outcomes can be described as interactions between resources and stressors and how they affect the individual (Spini et al., 15). This can include "personal distress, downward-leading life conditions, and limited social participation and capability to live a valued life" (Spini et al., 8). Context refers to location and time, but can also include history, culture, politics, and other factors where applicable (Spini et al., 16). These four categories do not stand independent of one another. Influence and overlap between these are common and expected. For example, resources and context together might translate into stressors (Spini et al., 14). Recognizing this enables a greater understanding of what is behind civilians' vulnerabilities and victimization throughout cyber-attacks.

This framework was chosen because it is multidisciplinary in nature and considers general vulnerability, rather than focusing on physical human vulnerability. Spini's Vulnerability Framework was created across multiple social science disciplines rather than through a single lens (Spini et al., 7). This approach enables it to be applicable in multidisciplinary projects like this one. In addition, its exploration of general vulnerability rather than physical human vulnerability is

significant, because this project looks at passive and active cyber-attacks that do not necessarily have direct physical effects on civilians in the way that kinetic attacks on civilians do. Instead, this vulnerability framework enables this project to explore civilians' vulnerability when there has not necessarily been direct physical harm, but rather their data or the confidentiality thereof has been affected.

Case Studies

As stated, this project looks at cyber-attacks in developed and developing countries to demonstrate that civilians are increasingly vulnerable to attacks regardless of their prosperity, their country's perceived security, and geographic location. These case studies, which include passive and active attacks in developed and developing countries, provide a variety of contexts to demonstrate various civilian vulnerabilities and victimizations. To review, these four cyber-attacks will serve as individual case studies to explore this vulnerability and victimization:

(1) The Anthem Cyber-Attack in the United States, which collected information from civilians in a developed country (Passive Attack).

(2) WannaCry Ransomware on the National Health Service in the United Kingdom, which influenced civilian hospitals and medical services in a developed country (Active Attack).

(3) The Jasmine Revolution Cyber-Attacks in Tunisia, which collected information from civilians in a developing country (Passive Attack).

(4) The 2010 Natanz Uranium Enrichment Facility Cyber-Attack in Iran, which influenced a power plant in a developing country (Active Attack).

Together, these four case studies demonstrate that regardless of civilian prosperity, perceived national security, and geographic location, civilians are increasingly vulnerable to attacks as a result of growing interconnectivity.

The Anthem Cyber-Attack in the United States: A Passive Attack in a Developed Country

Numerous sources state that the Anthem Attack in the United States was one of the largest data breaches of the 21st century and the largest data breach in healthcare history (Armerding; California Department…; Harwell and Nakashima). *Anthem, Inc*., the second largest health insurer in the United States, discovered the breach on January 27, 2015 and reported it to their current and former customers and employees soon after in February (California Department…; Armerding). Investigations revealed that the attack began nearly a year before on February 18, 2014 (California Department…). The attack began "when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content" (California Department…).[7] Upon opening the email, malicious files were downloaded to the user's computer, providing the attackers remote access to it "and at least 90 other systems within the Anthem enterprise, including Anthem's data warehouse" (California Department…). Anthem's chief information officer said the breach was recognized "when a systems administrator noticed that a database query was being run using his identifier code although he hadn't initiated it (Matthews and Yadron). If the system administrator had not noticed this irregularity, the breach may have continued undetected.

Once detected, however, the attackers had access to the inner workings of Anthem for an entire year. During this time, the attackers were able to move through Anthem's network,

[7] Phishing attacks are a form of social engineering and fraud. They involve pretending to be a trustworthy entity in an electronic communication (often using forged emails or websites) in order to persuade users to disclose sensitive information.

compromising 78.8 million records of current and former customers and employees (California Department…; Matthews and Yadron). Of these, at least 12 million were minors (California Department…). These records included names, birthdays, home addresses, email addresses, income data, and social security numbers (Matthews and Yadron; Harwell and Nakashima). It is uncertain whether their medical records and financial details, including credit card and bank account numbers, were compromised as well (Matthews and Yadron). Still, within two weeks of discovering the breach, Anthem hired a consumer credit protection company "to offer credit protection services to all breach-affected customers for a two-year period" and "a credit protection solution" to all who were minors when the breach occurred (California Department…). These measures highlight the possibility that these records were indeed compromised.

In response to the breach, public and private agencies worked together to best determine who was behind the attack and why. The California Department of Insurance played a leading role in examining the breach and they stated in a press release that they were sure "with a significant degree of confidence that the cyber attacker was acting on behalf of a foreign government." According to the Washington Post, many suspect this foreign government to be China as they have repeatedly targeted American health care providers and insurance companies in the past (Harwell and Nakashima). Cybersecurity experts state that both state and non-state actors target private health data "for extortion, fraud, or identity theft" (Harwell and Nakashima). A chief security strategist at a cybersecurity firm says, "Health care records are the new credit cards. If someone gets your credit card number, you cancel it. If you have HIV, and that gets out, there's no getting that back" (Harwell and Nakashima). The loss of confidentiality regarding social security numbers through this cyber-attack heightens the threat of extortion, fraud, and identity theft further.

WannaCry Ransomware on the National Health Service in the United Kingdom: An Active Attack in a Developed Country

WannaCry ransomware was a worldwide cyber-attack that affected over 150 countries, encrypting files and demanding ransoms in the cryptocurrency, Bitcoin, that began at USD$300 but jumped up to USD$600 a few days after the attack first emerged.[8] As a worm, it spread around the world through the Internet and local networks, taking advantage of a security vulnerability in Microsoft Windows (Gazula, 86).[9] Months after the attack, numerous countries and private companies, including the United States, United Kingdom, and Microsoft, stated that they were "as sure as possible" North Korea was behind the attacks to circumvent the sanctions against them (Hopping and Walker). Although, the United Kingdom's National Health Service (NHS) was one of the first large and significant organizations affected by the ransomware, it is worth noting that it was not necessarily targeted but rather happened to fall into the net of victims (Kerner). With regard to the NHS, the attack began on May 12, 2017 when NHS staff opened a malicious email attachment, which immediately encrypted the computer's data and locked out users (Clarke and Youngstein, 409). Once in NHS's network, the worm traveled to other systems, launching itself further and locking users out along the way.

Once inside the NHS network, every computer system was at risk and most became unusable. As the worm spread, electronic notes, imaging systems, drug-prescribing systems, electronic tests and their results, patient trackers, refrigerators for dispensing blood, and more became inaccessible (Clarke and Youngstein, 409-410). Over 19,000 surgeries and appointments

[8] Ransomware is a type of malware that prevents a user from accessing certain files or the entire system until a ransom is paid. Ransomware blocks access through encryption. The ransom note often states that upon paying the ransom, the files/system will be decrypted. Decryption upon paying the ransom, however, is never certain.
[9] A worm is a malware that seeks out other connected devices and systems in a computer network and transfers itself to them. Each additional device acts as a launching pad to additional networks and devices.

had to be canceled, walk-in and emergency patients turned away, and ambulances forced to drive further to get patients help (Field; Clarke and Youngstein, 409- 410). Major hospitals were forced to close trauma, stroke, and heart attack centers (Clarke and Youngstein, 410). Overall, more than 16 medical facilities and additional general practices, health groups, and NHS related organizations were affected ("Major Ransomware…"). Non-affected hospitals even quarantined themselves by shutting down their own networks to protect themselves from the worm (Clarke and Youngstein, 409). In locking users out of the system, the ransomware also affected the hospitals' telephone networks ("Major Ransomware…"). This was the case for seven days until May 19, 2019 when a kill switch was found stopping the worm from locking devices and spreading further (United Kingdom…, 4).[10] In those seven days, WannaCry ransomware cost the NHS £92 million to clean up, excluding an additional £60 million investment to update the medical infrastructure (Field).

In addition to the ransomware's tremendous effects of locking medical staff out of their systems, there were additional vulnerabilities civilians could have been exposed to if the attack had not been suspended. The ransom note indicated that if the payment was not made after seven days, the encrypted files would have been deleted (Symantec Security…). Experts who looked at the WannaCry code, however, did not find anything that would have deleted encrypted files (Symantec Security…). With the kill switch being activated on the seventh day, it is something we cannot be sure of. In the event that files would have been deleted, it could have included civilian's medical records, tests, prescriptions, doctors' notes, and more.

[10] A kill switch shuts something down abruptly, usually in the event of an emergency.

The Jasmine Revolution Cyber-Attacks on Civilians in Tunisia: A Passive Attack in a Developing Country

In December 2010, protests in Tunisia began calling for "extensive economic and social change" from Tunisian President Zine El Abidine Ben Ali as a beginning to the Arab Spring (Gazula, 45). Among the protestors' demands was an end "to the government's repressive online censorship regime and freedom of expression" (Gazula, 45). In addition to swarming the streets with these demands, Tunisians also took to "internet forums, blogs, Facebook pages, and Twitter feeds" (Gazula, 45). This was made possible through "Tunisia's modern communications infrastructure, pervasive Internet access, and a completely digitized mobile phone network" (Gazula, 45). Although Tunisians had access to this technology, which helped them organize themselves and protect their communities, they were still at the will of the government and the government-run Internet Services Provider, AMMAR (Delany; Gazula, 45). While social media certainly played a tremendous role in enabling the Tunisian public to remove Ben Ali, social media also made civilians vulnerable and susceptible to attack. It is worth noting that both sides perpetrated attacks, but this project focuses on those attacks where civilians were targeted.

Those who protested the government and the country's living conditions used social media for numerous reasons and in turn, the Tunisian government took advantage of the human and technological vulnerabilities of their connectivity. As stated, the public used social media to express their discontent of the Tunisian government and living conditions. The subject of these discussions and forums naturally evolved into planning protests and disseminating protest information further (Gazula, 46). In response, Ben Ali's government developed a cyber-police force "that monitored online activity, blocked access to opposition websites, [and] hacked into e-mails" with the intent to limit "the free flow of ideas and information" (Sprusanky). To hack into

e-mails, Tunisian authorities carried out targeted phishing attacks on Tunisians who had openly criticized authorities (Gazula, 47). In doing so, they took advantage of the human vulnerability to fall victim to these attacks and the technological vulnerability to not realize an unauthenticated user as anyone but the account owner. Although this was a passive attack where attackers merely collected digital information, it not only made civilians vulnerable online, it made them physically vulnerable as well.

Through these phishing attacks, Tunisian authorities were able to successfully hack the account of their critics, including Facebook, Google, and Yahoo! accounts (Carr). With their critics' usernames and passwords, Tunisian authorities used these civilians' accounts to spy on them, eliminate their online criticism, and reveal their physical locations (Gazula, 47; Carr). These compromised accounts also revealed their networks of contacts, which likely assisted the efforts of Tunisian authorities to silence the opposition further (Carr). With this access to private information, individuals were identified and silenced (Carr). One can suspect that the government's access to their private information, physical locations, and network of contacts led to many becoming the political prisoners that Ben Ali and the national police force held (States News Service). Overall, while interconnected devices and the use of social media enabled the Tunisian public to take a stand, it was also the means by which many were targeted and likely imprisoned.

The 2010 Natanz Uranium Enrichment Facility Cyber-Attack in Iran: An Active Attack in a Developing Country

Stuxnet is the name of the malware and worm that carried out the cyber-attacks on the Natanz uranium enrichment facility and other Iranian nuclear facilities over a series of years. It is

worth noting that there were numerous versions of Stuxnet that affected different parts of Iran's nuclear weapons program, but this case study will focus on the version that attacked the Natanz uranium enrichment facility between 2009 and 2010.

This version of Stuxnet was first found in Iran in June 2009, but it did not reach the plant and carry out its payload until a year later (Broad). To reach the Natanz plant, Stuxnet began infecting companies that worked with Iran's nuclear program in one way or another, companies that manufactured their products, assembled components, installed industrial control systems, and more (Zetter). This was necessary for attackers to get the worm into Natanz, because its systems were closed off from public networks, a quality referred to as air-gapped (Zetter). The idea was that employees of these companies would unknowingly plug infected USB flash drives into Natanz computers to get the worm into the plant (Zetter). On June 23, 2010, the worm hit the first of these companies that would physically carry Stuxnet into the plant (Zetter). It is unknown when the attack reached its target, but by August of that same year 328 of Natanz's centrifuges were down (Zetter). This number grew to 984 centrifuges down by November 2010 (Zetter). In addition, additional centrifuges that had been installed were not being fed gas (Zetter). It is unknown whether this was a human decision or whether Stuxnet played a direct role in limiting the flow of gas as well. Although the plant had 3,936 centrifuges still functioning after the cyber-attack, Stuxnet still altered and destroyed many systems without the victim aware that they were being deliberately attacked for over a year (Zetter). In doing so, the plant's capacity was successfully reduced.

Stuxnet functioned by taking advantage of known vulnerabilities, known as zero-day vulnerabilities, in a software known as Siemens Step7. This software is "used to program industrial control systems that operate equipment," including nuclear centrifuges (Kushner; Gazula, 31).

Once one of the infected employee USBs, carrying the Stuxnet worm, was plugged in at the plant, the worm was able to make its way to the Siemens software and manipulate it "to speed up or slow down the centrifuges causing them to destroy themselves" (Gazula, 31). The malware was even able to act "without showing any signs of problems on monitoring systems" (Gazula, 31). In other words, not only did the plant operators not know that they were being attack, their monitoring systems did not even report that the centrifuges were malfunctioning. Instead, the malware "recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators" while the centrifuges actually tore themselves apart (Broad). Even if the operators noticed the disruption, the worm was also coded to stop a safe plant shutdown that would prevent the centrifuges from destroying themselves (Broad).

To make matters worse, the Stuxnet worm was uncontained, which affected other users' systems around the world and could have potentially caused great damage to unintended targets as well if not for its expert coding. As a worm, Stuxnet had an intended day of death, meaning the day when the worm was supposed to stop spreading, which was set for June 24, 2012 (Knopová and Knopová, 28). However, Stuxnet was found still conducting attacks on December 25, 2012, indicating either some error or an alteration (Knopová and Knopová, 28). Additionally, while Stuxnet was not intended to travel outside of the Iranian nuclear program, it did when one of the infected employees connected their laptop to the Internet (Manzo). By these means, Stuxnet reached all corners of the world, including India, Indonesia, and many others (Broad). In one confirmed case, Chevron reported that Stuxnet was found spreading "across its machines" in the United States (Kushner). Only thanks to Stuxnet's expert coding, which is suspected to come from the United States and Israel, was it "engineered to affect Iranian enrichment facilities only" (Manzo). If less skilled programmers had attempted such a feat without specifically targeting

certain machines, the destruction could have been as uncontained as the worm itself, destroying machines and erasing data around the world.

Moving forward, the attackers' success might act as motivation to carry out additional attacks or for others to copy these attacks against their own enemies, whether this be between state, non-state, or both types of actors. Accordingly, experts in the field say, "Regular cybercriminals look at something that Stuxnet is doing and say, that's a great idea, let's copy that," (Kushner). Although this attack was on a suspected national nuclear weapons program, a civilian plant could easily be targeted in the same way by any type of opposition, whether it be a foreign state, host state, foreign non-state actor, or host non-state actor. Industrial machines, specifically, are of great vulnerability and the known vulnerabilities in the Siemens software are examples of that (Kushner). Not only are many industrial control systems "hooked up to the Internet," but many do not "change the default password" to the control panels, nor do they update these controls (Kushner). Cybersecurity firms have even found "critical infrastructure companies running 30-year-old operating systems" (Kushner). This translates into either widely known vulnerabilities or systems where support is no longer provided, meaning vulnerabilities are left unpatched. By these means, attacks identical to Stuxnet and the Natanz uranium enrichment facility can easily be carried out against civilian plants and other significant infrastructure.

Analyses of Civilian Vulnerability According to Spini's Vulerability Framework

These four cyber-attacks negatively impacted the lives of civilians and worsened their vulnerability to future attacks, regardless of civilian prosperity, perceived national security, and geographic location. The vulnerability of civilians to such attacks, and their victimization during and afterward, will be dissected according to Spini's Vulnerability Framework. In most cases, upon being victimized by cyber-attackers, these civilians are increasingly vulnerable to further

attack. This framework looks at resources, stressors, outcomes, and contexts to explore this cycle of vulnerability and victimization. In analyzing these cyber-attacks according to Spini's Vulnerability Framework, I created tables to organize the analysis of civilian vulnerability according to these factors. To organize this analysis further, I look at these factors during and after the attack separately. This will demonstrate that civilian prosperity, perceived national security, and geographic location are not necessarily safeguards against cyberwarfare and cyber-attacks. Although developed countries seemingly have more cybersecurity resources and protections, their civilians are equally susceptible to being the victims of cyber-attacks just as civilians in developing countries. As such, civilian vulnerability and victimization is only increasing internationally as a result of growing interconnectivity.

To measure civilian vulnerability, this project uses the definition of vulnerability from Spini's Vulnerability Framework. As previously stated, the creators of this framework define vulnerability as:

> "…a lack of resources, which in a specific context, places individuals or groups at a major risk of experiencing (1) negative consequences related to sources of stress; (2) the inability to cope effectively with stressors; and (3) the inability to recover from the stressor or to take advantage of opportunities…" (Spini et al., 19).

With this definition, vulnerability can be explored as both a state and a process. Spini writes that vulnerability can also be seen as a "process of weakening" that depends on a "stressful event or symbolic threat [that] appears in the life of the person" (Spini et al., 19). Spini writes on that "…vulnerable individuals will have difficulties in coping effectively with the stressor and manifest outcomes of vulnerability will emerge" (Spini et al., 19). This project also highlights how this growing vulnerability naturally evolves into further victimization, either possible or confirmed after each cyber-attack.

The Anthem Cyber-Attack in the United States: A Passive Attack in a Developed Country

As stated, the Anthem cyber-attack was a passive attack on the second largest health insurer in the United States, a developed country. This attack compromised the confidentiality of 78.8 million records of current and former Anthem customers and employees, at least 12 million of which were minors (California Department…; Matthews and Yadron). These compromised records included names, birthdays, home addresses, email addresses, income data, social security numbers, and possibly medical records and financial details as well, including credit card and bank numbers (Matthews and Yadron; Harwell and Nakashima). Spini's vulnerability framework helps lay out the vulnerabilities and victimizations of the attacked civilians throughout the cyber-attack.

There were a series of resources, stressors, outcomes, and contexts for the attacked civilians that were constant throughout the Anthem attack, from before the attack even occurred until long afterward (Table 1.1). Regarding resources, civilians had their personal coping strategies, social networks, and support systems throughout the attack. Civilians also had the Anthem information security department and staff supposedly working to protect the confidentiality of their information. According to Spini, an abundance of these resources can help reduce vulnerability, while a lack thereof may increase their vulnerability as these resources help civilians cope with stressors, outcomes, and contexts. As customers of a health insurer, possible stressors these civilians may have endured throughout the attack included health conditions, an inability to study or work due to health concerns, or maintaining good health. In addition to the attack and breach of confidentiality, large stressors like health conditions increase one's vulnerability. Because of these stressors, a potential outcome for these civilians is nervousness regarding their health. Throughout the attack itself, a potential need for medications, accomplishments in life, and bills are context that contribute to vulnerability as well, because these matters have lost their confidentiality.

Additional context includes their economic status or prosperity, and where the attack occurred, which depicts perceived national security and geographic location. These factors depict civilian vulnerability throughout the attack from before it even began until afterward when the attack finished.

Table 1.1

Spini's Vulnerability Framework Factors	Constants Throughout the Anthem Cyber-Attack
Resources	Coping strategies, social networks, and support systems. Anthem's information security department and staff on site.
Stressors	Health conditions, inability to study or work due to health concerns, or maintaining good health.
Outcomes	Nervousness regarding health.
Context	Economic status (civilian prosperity), necessary medications, accomplishments, bills and purchases. State where attack occurred (perceived national security and geographic location).

Spini's framework also helps identify factors during the Anthem cyber-attack that depict civilian victimization and vulnerability (Table 1.2). Although there were no new resources, stressors, and outcomes during the attack, there was significant context: civilians were unaware of the ongoing attack for over a year (February 2014 through February 2015). This is central to understanding the reaction that follows when civilians find out their information has been under attack for over a year without any hint to the owners of this context. Throughout that year, civilians may have never even questioned the security of the information, while an unknown attacker was collecting everything from their names to addresses to social security numbers. When the attack was finally detected, civilians' vulnerability and the possibility for future victimization grew.

Table 1.2

Spini's Vulnerability Framework Factors	During the Anthem Cyber-Attack
Resources	
Stressors	
Outcomes	
Context	Unaware of the ongoing attack.

Once the attack was detected and the breach was put to an end, additional factors came into play increasing civilian vulnerability (Table 1.3). Unlike the other three cyber-attacks, the Anthem cyber-attack was the only case where civilians gained access to additional resources when Anthem paid for financial and security resources to those civilians affected by the breach. Although this may have been helpful, the list of stressors grew through a victimization-vulnerability cycle following the cyber-attack. With their information no longer confidential, the chances of extortion, fraud, and identity theft, and the chance of another breach in the future creates stressors for civilians as well. With these stressors, the list of outcomes grows as well. Civilians may grow nervous regarding their information's security and may question the ability of organizations to protect their information. In addition, civilians may worry that the attack might affect Anthem's ability to provide its products and services, because of the economic costs to clean up the breach and the reputational damage. The context of civilians having just been victimized contributes to their vulnerability as well as they must cope with it.

Table 1.3

Spini's Vulnerability Framework Factors	After the Anthem Cyber-Attack
Resources	Financial resources, security resources.
Stressors	The attack itself, loss of information's confidentiality. Possible extortion, fraud, and identity theft. The chance of it happening again.
Outcomes	Nervousness regarding information's security. Lack of trust and confidence in others and organizations. Worry that this attack may economically affect Anthem's products and services.
Context	Having just been victimized.

These factors throughout the Anthem cyber-attack depict the vulnerability and victimization of affected civilians. Although Anthem offered financial and security resources after the attack, there was still a pressing list of stressors not limited to health conditions and the possibility of impending extortion, fraud, and identity theft. In addition, the outcomes regarding personal distress and a lack of trust in organizations moving forward may prevent civilians from effectively coping with their stressors. This personal distress and lack of trust can in turn prevent civilians from taking advantage of opportunities to better their situations as they struggle to cope and recover (Spini et al., 8). In not being able to cope or recover, Spini states that these individuals are at risk of "downward-leading life conditions," "limited social participation," and a reduced "capability to live a valued life" (Spini et al., 8). In doing so, civilians grow increasingly vulnerable in fulfillment of Spini's definition of vulnerability.

Despite living in the United States, millions of civilians lost the confidentiality of their electronic records. The prosperity of civilians relative to civilians in other states, the elite cyber protections put in place by both the government and private organizations, and the geographic location did not protect these civilians. Instead, they were victimized by attackers whose identity remains uncertain and have grown in vulnerability as demonstrated by the analysis of the factors that comprise Spini's Vulnerability Framework. In turn, these vulnerabilities grow into means of victimizing these civilians further through extortion, fraud, and identity theft.

WannaCry Ransomware on the National Health Service in the United Kingdom: An Active Attack in a Developed Country

The encryption and unavailability of systems that resulted from WannaCry ransomware when it entered the network of the United Kingdom's National Health Services affected thousands

of civilians. In accordance with Spini's Vulnerability Framework, the four factors of resources, stressors, outcomes, and context throughout the WannaCry ransomware cyber-attack depict civilian vulnerabilities and potential future victimizations. As an active attack—which manipulates information and often, has a secondary purpose that influences the real world—the WannaCry ransomware cyber-attack had these noticeable implications as soon as the cyber-attack began.

First, the constant resources, stressors, outcomes, and context of affected civilians depict their scenarios throughout the WannaCry ransomware cyber-attack from before the attack even began until long after it ended (Table 2.1). As resources, civilians had their personal coping strategies, social networks, and support systems to help them navigate their stressors. Throughout the cyber-attack, the NHS England IT department and staff also offered whatever help they could with computer systems and networks. Much like the Anthem attack, constant stressors included potential health conditions, an inability to study or work due to health concerns, or the maintenance of good health. Because of these stressors, a natural outcome throughout the attack was likely nervousness regarding their health. In addition to economic status/civilian prosperity and the state where the attack occurred, an ongoing, constant context of affected civilians may have included needed prescriptions and medications as well, that suddenly became unavailable during the attack. While these factors were constant throughout the attack, other factors are unique to the period in which the attack was underway.

Table 2.1

Spini's Vulnerability Framework Factors	Constants Throughout the WannaCry Ransomware Cyber-Attack
Resources	Coping strategies, social networks, and support systems. The NHS England IT department and staff.
Stressors	Health conditions, inability to study or work due to health concerns, or maintaining good health.
Outcomes	Nervousness regarding health.
Context	Economic status (civilian prosperity), necessary medications. State where attack occurred (perceived national security and geographic location).

As an active attack, WannaCry ransomware impacted civilians directly; in this case, as soon the malware hit computer systems (Table 2.2). Unlike the Anthem Attack, civilians did not gain access to additional resources while under attack. Instead, during the cyber-attack there was a surge of stressors including the attack itself, which involved thousands of cancelled surgeries and appointments, unavailable prescription mechanisms, unavailable emergency centers, and countless other unavailable services. With these stressors, civilian outcomes potentially included fear regarding the attack and fear regarding the event of needing emergency care that is unavailable or of reduced quality. At the same time, civilians endured the context of being victimized, unsure of how long this attack will last and with that, how long systems will be down. When the attack did end, however, additional factors that contribute to their vulnerability and possible future victimization came into play as well.

Table 2.2

Spini's Vulnerability Framework Factors	During the WannaCry Ransomware Cyber-Attack
Resources	
Stressors	The attack itself, cancelled surgeries and appointments, unavailable prescription mechanisms, unavailable emergency centers, unavailable services.
Outcomes	Fear regarding the attack and the possibility of needing emergency care that is unavailable or reduced quality.
Context	Being victimized. The uncertainty of how long it will last.

Once the kill switch was found and the damage cleaned up, the attack was not necessarily over; it had lingering effects especially on affected civilians (Table 2.3). Although civilians could be attended to once again as patients, they continued to only have their own personal resources to cope with the stress of the attack. As stressors, civilians have to deal with the possibility of a similar attack occurring again and to make matters worse, potentially not finding a kill switch in time, leading to the deletion of encrypted data, the attack spreading further, or the attack being altered and worsened. Once civilians began to settle down after the attack, outcomes might have included a lack of trust and confidence in the National Health Service to ensure availability of quality healthcare and in the United Kingdom's general ability to keep its civilians and infrastructure safe. The civilian context after the WannaCry ransomware attack would have been that of only recently being victimized. These factors translate into civilians' unique vulnerability throughout such an attack.

Table 2.3

Spini's Vulnerability Framework Factors	After the WannaCry Ransomware Cyber-Attack
Resources	
Stressors	The chance of it happening again and in the future, not finding a kill switch in time.
Outcomes	Lack of trust and confidence in the National Health Service to ensure availability of healthcare and in the United Kingdom's security overall.
Context	Having just been victimized.

Together, all of these factors not only demonstrate how civilians were victimized throughout the WannaCry ransomware cyber-attack, but also how they are vulnerable moving forward. Unlike after the Anthem cyber-attack, where civilians were provided specialized resources relevant to the ways in which they were attacked, sources do not suggest that civilians in the WannaCry ransomware attack were offered any additional resources for dealing with the

stressor of unavailable healthcare. This lack of resources worsens the severity of stressors for civilians unable to deal with them. For example, during the attack, someone's lack of resources may have prevented them from driving further to receive necessary healthcare. Recognizing this lack of resources, may leave civilians unable to recover from aforementioned stressors and their outcomes, such as the fear of such an attack happening again, and a lack of faith in the NHS and British government to serve civilians as intended. According to Spini, this personal distress regarding a future attack and a lack of trust in the NHS and British government may lead individuals to additional suffering due to their lack of resources to deal with such stressors and outcomes.

Despite living in a prosperous and seemingly secure state, these civilians were attacked and made vulnerable in not having access to healthcare for a period of seven days. Although this is the case in countless places around the world, it is a tremendous anomaly in one of the world's leading economies and social environments. Without resources to reduce these vulnerabilities, civilians in developed, seemingly secure state are growing increasing vulnerable to attack.

The Jasmine Revolution Cyber-Attacks on Civilians in Tunisia: A Passive Attack in a Developing Country

As stated, the Jasmine Revolution cyber-attacks began with the Tunisian government hacking civilians' social media accounts and with this access led to events ranging deleted posts to civilians being physically located to civilians likely being imprisoned as political prisoners. Because these were passive attacks, similar to the Anthem cyber-attack, the effects were primarily noticeable afterward. Still, there were significant factors present throughout.

Constant factors throughout the Jasmine Revolution cyber-attacks depict the lives of the affected civilians (Table 3.1). Naturally, civilians' resources included their personal coping strategies, social networks, and support systems throughout the attack. Tunisia's telecommunication networks held a significant role in upholding many of these support networks and so these networks were a significant resource as well (Delany). Still, like the WannaCry ransomware attack, civilians at no point were provided additional resources to deal with the hackings and the physical locating of critics that followed. Their stressors, however, were tremendously distinct from those of the other cyber-attacks. The Tunisian cyber-attacks occurred during the Jasmine Revolution, which was a national revolution with a range of demands. Economic despair was both a source of numerous demands and a worsening context that acted as a stressor as well. An additional stressor was the fact that the national police force was arresting political prisoners throughout the course of the cyber-attacks and revolution overall. With these stressors, civilian outcomes naturally involved fear and desperation regarding their daily lives and the lack of security. The context of the time involved a lack of civilian prosperity due to the economic despair, the ongoing national revolution, and the state where the attack occurred, which in this case depicts the lack of security and the close proximity between the attackers and victims. This close proximity between the attackers and victims is unique to this case study, depicting a distinct set of civilian vulnerabilities to nearby attackers. These factors were present throughout the Jasmine Revolution cyber-attacks from before they occurred until after they had finished.

Table 3.1

Spini's Vulnerability Framework Factors	Constants Throughout the Jasmine Revolution Cyber-Attacks
Resources	Coping strategies, social networks, and support systems. Tunisia's expansive telecommunication network and resources.
Stressors	A national revolution, economic despair, national police force arresting political prisoners.
Outcomes	Fear and/or desperation related to their stressors.
Context	Economic status (a lack civilian prosperity), ongoing national revolution. State where attack occurred (perceived security and geographic location).

As a series of passive attacks, their effects were minimal while they occurred (Table 3.2). During the attacks, affected civilians may have been frustrated with deleted posts and unavailable websites as outcomes of the cyber-attacks. Despite these deleted posts and unavailable websites, civilians had no way of being sure that this was an attack or a legitimate technical difficulty, like websites being down for bandwidth reasons.[11] This was the context during the cyber-attacks: uncertainty regarding technical occurrences. Still, it is likely that many Tunisians suspected the government was behind these attacks as a part of their two-way cyber-battle (Delany). Unlike the Anthem cyber-attack, however, which only had the possibility of leading to future attacks, the Jasmine Revolution cyber-attacks led to confirmed follow-up attacks. In other words, as a result of civilians being victimized, the Jasmine Revolution cyber-attacks created further vulnerability that affirmatively resulted in further victimization.

Table 3.2

Spini's Vulnerability Framework Factors	During the Jasmine Revolution Cyber-Attacks
Resources	
Stressors	
Outcomes	Frustration with deleted posts and unavailable websites.
Context	Uncertain if this was an attack or a legitimate technical difficulty.

[11] Bandwidth is a measure of the information-carrying capacity of a channel.

Once the Jasmine Revolution cyber-attacks finished being conducted, the victimization of these cyber-attacks was followed by further vulnerability that the Tunisian government took advantage of (Table 3.3). As stated, affected civilians did not have access to additional resources specific to the stressors they were facing. Considering Tunisia was undergoing a national revolution, it is understandable that resources were scarce if existent at all. With regard to stressors after the cyber-attacks, civilians faced government authorities locating, silencing, and—one can deduce—arresting those who opposed authorities. It is possible that after these attacks, the possibility of similar cyber-attacks by future authorities would act as stressors to affected civilians and other Tunisians as well. Meanwhile, outcomes may include civilians lacking clarity of how they were identified and located. If they themselves were not attacked, but witnessed someone else who was, civilians may fear that they will be next in being persecuted by authorities, becoming the victims of extortion, or being arrested as political prisoners. An additional outcome may be that civilians distrust future authorities as a result of this breach of confidentiality. The range of events from deleted posts to experiencing the arrest of political prisoners depicts the context unique to the cyber-attacks. These factors help portray the vulnerabilities of affected civilians after the Jasmine Revolution cyber-attacks in Tunisia.

Table 3.3

Spini's Vulnerability Framework Factors	After the Jasmine Revolution Cyber-Attacks
Resources	
Stressors	Government locating, silencing, and arresting those who oppose authorities. The possibility of future authorities conducting similar attacks.
Outcomes	Lack of clarity regarding how they were identified and located. Fear that they may be hacked, persecuted, extorted, or arrested next. Lack of trust in future authorities.
Context	Having themselves or a friend victimized.

Together, these factors depict the range of vulnerabilities civilians faced throughout the Jasmine Revolution cyber-attacks in Tunisia. With the context of Tunisia already stressful as it was at the time, the cyber-attacks added additional stressors and outcomes for civilians to face. All of these factors increased civilian vulnerability exponentially. In addition to the ongoing revolution, the cyber-attacks enabled authorities to locate civilian critics to silence them and likely arrest them, increasing civilian vulnerability further. The lack of resources and growing list of stressors led to negative outcomes, which in the long term have the potential to inhibit civilians' ability to cope effectively and recover from these events as Spini suggests (Spini et al., 19). Although many Tunisians continued to use social media after the attacks, some civilians may struggle to recover from stressors, such as the fear of these events repeating themselves. Without recovering from these stressors, it is possible that these affected civilians may limit themselves in the opportunities they encounter in an effort to protect themselves from further cycles of vulnerability and victimization.

The 2010 Natanz Uranium Enrichment Facility Cyber-Attack in Iran: An Active Attack in a Developing Country; and the Possibility for an Identical Attack on a Civilian Power Plant

Although the 2010 Natanz uranium enrichment facility cyber-attacks were conducted on what is suspected to be a plant for a national nuclear weapons program, this example depicts how an identical attack could be carried out against a civilian power plant. This analysis explores the vulnerabilities of civilians if a civilian hydroelectric plant that powers a city in a developing country came under attack in the same way as the Natanz facility. As with the Natanz facility, where about a quarter of centrifuges were destroyed, this example mirrors that with the possibility of an attack where some of the hydro-turbines are targeted and destroyed, reducing the capacity of

the plant until they are replaced, much like the Natanz plant. Naturally, the resources, stressors, outcomes, and contexts of the attack may differ from place to place, but this analysis hopes to best capture the vulnerability of civilians in such a case, and the possibility of further victimization.

Just as with the other case studies, there would be factors present throughout the civilian power plant cyber-attacks from before they even happen until after they have finished (Table 4.1). Constant resources would include civilians' personal coping strategies, social networks, and support systems. Stressors may depend on the presence of conflict or grievances or any national or regional divisions or political issues. The outcomes of these stressors and resources may involve the opinions regarding opposing groups in the country, region, or internationally. Context would involve average to heavy reliance on the plant for electricity and the assumption that the country has a developing electrical grid. This suggests that in the event that the plant goes down, there may not be the option to reroute extra energy from another plant into this part of the grid. Local and national politics, history, civilian economic status, and the location of where the attacks occur are also considered contextual factors that impact civilians' vulnerability.

Table 4.1

Spini's Vulnerability Framework Factors	Constants Throughout Civilian Plant Cyber-Attacks
Resources	Coping strategies, social networks, and support systems.
Stressors	Conflict or grievances. National or regional divisions or politics.
Outcomes	Opinions regarding opposing groups in the country, region, or internationally.
Context	Reliability on the plant for electricity. Local and national politics, history. Economic status (civilian prosperity). State where attack occurs (perceived national security and geographic location).

As stated, this civilian power plant cyber-attack would mimic the Natanz facility cyber-attack in the way in which the attack reduced the plant's capacity (Table 4.2). With some hydro-turbines of the hydroelectric plant down, the plant's ability to provide energy to the civilian

electrical grid would be affected. One possible response is that civilians who have only recently begun having electricity may not have a problem reverting to some of the ways in which they used to do things. However, civilians who have become accustomed to having electricity may see it as a disturbance to daily life. As stated, a developing country may or may not have the resources to help civilians cope with such a disturbance. For these individuals who have become accustomed to having electricity, the inconsistence or absence thereof may act as a stressor, especially if it inhibits civilians' ability to go to school or work. If it is known that it is an attack, the attack itself would act as a stressor as well. The outcomes of this may involve frustration or annoyance with the lack of electricity and interruption to daily life. If it is known that it is an attack, civilians might also become upset with their enemies whether or not the perpetrator's identity has been confirmed. In other words, civilians might jump to the conclusion that some group whom they oppose is behind the attack with the intention to inhibit them. On the other hand, civilians and plant operators may be unaware that this is an attack and may simply consider it a legitimate technical difficulty. By these means, a cyber-attack on a civilian power plant victimizes civilians as such and opens them to further vulnerability according to Spini's Vulnerability Framework.

Table 4.2

Spini's Vulnerability Framework Factors	During Civilian Plant Cyber-Attacks
Resources	
Stressors	Inconsistent or absent electricity. Inability to go to school or work. If it is known that this is an attack, the attack itself.
Outcomes	Frustration or annoyance with the lack of electricity and interruption to daily life. If it is known that this is an attack, civilians might become upset with their enemies whether or not the perpetrator's identity has been confirmed.
Context	On the other hand, civilians and plant operators may be unaware that this is an attack.

After the cyber-attacks on the civilian power plant have concluded in the same way as the cyber-attack on the Natanz facility, the reduced capacity of the plant would continue until the damaged pieces are replaced (Table 4.3). Due to this occurring in a developing country, it may be difficult to offer resources to civilians due to low economic funds that must now manage the damages as well. With regard to stressors for civilians, a reduced availability of electricity could potentially lead to a reduced quality of goods and services as well. The possibility of this happening again and worsening the availability of electricity further would also act as a stressor for civilians. As a result of these stressors and the lack of resources to assist civilians, one expected outcome would be a lack of trust in the plant to provide electricity reliably. With time, an additional outcome could be that if it is known that this is an attack, civilians' anger with enemies might escalate whether or not the perpetrator's identity has been confirmed. On the other hand, civilians and plant operators may continue to be unaware that this is an attack and leave these vulnerabilities unpatched. This in turn would lead to greater vulnerability and victimization as attackers have already successfully carried out the attack once and may do so again.

Table 4.3

Spini's Vulnerability Framework Factors	After Civilian Plant Cyber-Attacks
Resources	
Stressors	Reduced availability of electricity, leading to reduced quality of goods and services. Chance of this happening again and worsening the availability of electricity further.
Outcomes	Lack of trust in the plant to provide electricity reliably. If it is known that this is an attack, civilians' anger with enemies might escalate whether or not the perpetrator's identity has been confirmed.
Context	On the other hand, civilians and plant operators may continue to be unaware that this is an attack and leave these vulnerabilities unpatched.

Overall, these factors demonstrate civilian vulnerability in the event of a cyber-attack on a critical civilian power plant. If the infrastructure does not exist to provide resources to civilians post cyber-attack, this may simply exacerbate new and ongoing stressors, which in turn worsens outcomes, and cultivates further vulnerabilities. As stated previously, if unable to cope with their stressors and outcomes, civilians may never recover from them, leaving these civilians with residual scars from these attacks. In the long term, this can also limit civilians' willingness to partake in new and beneficial opportunities as suggested by Spini (Spini et al., 19). As a result, civilians may endure long-term cycles of vulnerability and victimization. In the event of such an attack or a series thereof on critical infrastructure in a developing country, communities may struggle or be completely prevented from developing and improving their living standards. By these means, interconnected devices and networks are increasing civilian vulnerability and victimization to an extent not seen so dramatically before.

Similarities across these Cyber-Attacks: A Lack of Resources

It is evident that there are similarities across these cyber-attacks during their occurrence and afterward. Among these is the significance of resources to help civilians cope with their stressors and in turn, prevent or at least reduce their outcomes as suggested by Spini (Spini et al., 19). The availability of effective resources however, is lacking, regardless of civilian prosperity and where the attacks occur. Although Anthem did provide its customers and employees financial and security services after its cyber-attack, neither the National Health Service nor the United Kingdom offered its civilians any assistance after the WannaCry ransomware debilitated healthcare services across the United Kingdom for seven entire days. This is a major concern. If resources and assistance are not consistently provided in leading economies and countries, then

civilians in developing countries may receive little, if any attention, when they need assistance after a cyber-attack, like the cases in Tunisia or in the possible case of a cyber-attack on a critical civilian power plant in a developing country or region. At the same time, while Tunisian telecommunication networks benefitted the Tunisian public in the Jasmine Revolution overall, it did not prevent authorities from silencing and potentially locating individuals to arrest them as political prisoners. This demonstrates that interconnectivity may indirectly enable crime and human rights violations as well. These are concerns regarding civilian vulnerability and victimization that need to be addressed not only in the field of cyber security, but naturally in political science and humanitarian studies as well. Without these considerations, however, civilians become increasingly susceptible to attack regardless of civilian prosperity, perceived national security, and geographic location moving forward.

Conclusion

The creation of cyberspace with increasingly connected devices, services, infrastructure, and more has resulted in an additional front for enemies to fight battles. They are no longer limited to air, land, and sea, making distance and cost of decreasing significance. Cyberspace and increasing connectivity allows attacks to be conducted without regard for prosperity, traditional notions of security, and geographic location. At the same time, because civilians and governments share the same basic networks, malwares attack these two without preference for one over the other. In other words, even if the attacker intends to solely attack a military target, the sharing of these networks leaves civilians vulnerable to the same attack, especially if the malware is uncontained like the Stuxnet worm, which was intended for the Natanz uranium enrichment facility, but was found in many other places as well. In the event that the intended targets are

indeed civilians, interconnectivity makes these attacks easy. Cyber-attacks are inexpensive in relation to traditional weapons, do not require much expertise, and can be conducted from anywhere in the world through computer networks. The ease of these attacks drastically increases civilian vulnerability and in turn, increases civilian victimization without regard for their prosperity, perceived national security, and geographic location. This is exemplified in detail through the conducted analysis and translates into a fundamental change in what we know about security.

In looking at civilian resources, stressors, outcomes, and contexts as per Spini's Vulnerability Framework, the cycle of vulnerability and victimization due to increased interconnectivity becomes evident. Although technology certainly enables a great deal of possibilities to better living standards, such as improved healthcare and the ability to disprove rumors, technology is also constantly on the defensive and susceptible to attack. The susceptibility of technology to attack makes civilians directly and indirectly vulnerable as they grow increasingly connected and come to rely on interconnected devices. With increased vulnerability, increased victimization naturally follows. Although Tunisians were able to fight back through social media in the greater context of the Jasmine Revolution by disproving government rumors, the proximity of attackers and victims played a tremendous role in allowing that to happen. When attackers and victims are oceans apart, such as in the other three case studies, how can civilians retaliate against attackers? How can civilians protect their information and infrastructure? With cybercriminals constantly identifying news methods of conducting attacks, potential victims can only hope their defenses are up to the task. In other words, those on the defensive can only hope they are able to minimize the always-present gap of vulnerability. This lack of certainty depicts civilians' growing vulnerability that allows for victimization.

Overall, factors related to civilian prosperity, perceived national security, and geographic location offer little, if any solace, to civilians' vulnerability to and victimization through cyber-attacks. The United States' Anthem and the United Kingdom's National Health Service both had security protocols in place and IT staff behind them and yet civilians were tremendously victimized and became increasingly vulnerable to further attack. In Tunisia, meanwhile, connectivity did enable civilians throughout the Jasmine Revolution, but their connectivity was used against them for the sake of silencing and tracking. If the victims and attackers had not been as close as they were, perhaps civilians would not have been as successful overall in protecting themselves. Finally, in the event of a civilian power plant cyber-attack similar to the Natanz uranium enrichment facility attack, a country's development could be set back by repeatedly attacking their developing infrastructure. These four case studies demonstrate that civilians are vulnerable around the world regardless of their context. Although attackers will always do as they please to achieve their goals, the international community still ought to make strides to reduce civilian vulnerability and modify acceptable standards of behavior that consider cyber-warfare and potential developments to come. By these means, there would be incentives to reduce collateral damage and an expectation to punish those who do not abide.

Moving Forward

In conducting this research, numerous questions came to mind that could be explored further. Addressing these questions would benefit civilians and those who work to reduce their vulnerability and increase security overall. Among these is the matter of geographic location and proximity. Geographic location was a significant factor in this project in the sense that I argued it no longer served as a safeguard for those targeted by attackers. However, the Tunisian case study

of the Jasmine Revolution cyber-attacks presented an interesting case. Of the four case studies, this is the only one where the victims and attackers were within close proximity to one another. Because of this proximity, the information collected from the passive attack was immediately used to conduct in-person attacks, specifically locating and likely imprisoning civilian critics. Beyond the scope of this project, the close proximity also allowed civilians to counter some of the rumors the government was spreading, enabling civilians to effectively take a stand against their cyber-attackers. Is this scenario limited to events where victims and attackers are within close proximity? Exploring this matter of how increased connectivity leads to both increased vulnerability and an increased ability to fight back would make for interesting further research.

This project loosely touched upon three other topics that would make for interesting further research as well. The first of these is with regard to the differences between targeted attacks on specific individuals and attacks on a larger group or society. These differences can be explored in today's attacks or in possible future attacks. With this, further research is endless and can explore the strategy and motive of past attacks and where and how we can expect future attacks on either of these targets. At the same time, cybersecurity experts have noted that cybercriminals often copy code from successful cyber-attacks for their own intents and purposes. Further research regarding the frequency and success of copycat attacks would be valuable from a security perspective and could highlight how civilian vulnerability goes beyond those initially targeted, creating a type of domino effect. In contrast, it would also be interesting to see how the advancement of cyberspace compares to previous military advancements, like nuclear weapons, and the vulnerability of civilians over time. By researching these matters and exploring them further, societies can better protect civilians' vulnerabilities today and moving forward.

Alongside further research, international and domestic communities must also acknowledge these vulnerabilities and work to reduce them and their effect on civilians. Effectively reducing civilian vulnerability overall, however, is difficult due to the massive numbers of stakeholders. Although some organizations have gathered national leaders to discuss cybersecurity, not limited to the United Nations, the European Union, and the African Union, private manufacturers, engineers, and enforcement agencies must do their part to keep consumers secure (Talihärm). In other words, while national and international communication is beneficial, without implementation, these efforts do little to reduce vulnerability. Without comprehensive involvement of stakeholders, there will be holes through which attackers can easily target civilians. As discussed earlier in this paper, efforts to reduce costs almost always result in reduced security. Although there will always be security gaps due to oversight or the desire to cut costs, communities must effectively work to reduce civilian vulnerability by minimizing gaps in security. As long as these gaps do exist, providing resources appropriate to varying contexts following cyber-attacks can help civilians cope and move forward after victimization. By these means, the cycle of civilian vulnerability and victimization can begin to be managed and hopefully reduced overall.

In addition to such efforts to limit the means by which attacks can be conducted and affect civilians, national and international actors must continue to identify unacceptable behavior and stop those responsible to reduce further vulnerability and victimization. Although the facilitation of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was not intended to have the force of the law, it is an appropriate step to clarify where cyber-warfare stands in current international law. With this clarity, national and international actors can begin making considerations and adjustments where necessary to reduce cyber-criminals slipping through the

cracks of justice. While some cyber-criminals may always slip through, actions need to be present to reduce the likelihood that they will further cycles of civilian vulnerability and victimization.

Bibliography

Akarcay, Pinar, and Gökhan Ak . "Rethinking Cyber Warfare: Timeless, Normless and Unconstrained." *IKSAD Journal*, vol. 4, no. 9, 2018, pp. 195-214. http://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1273703&dswid=-4885.

Aleinikoff, T.Alexander. "The Present, Past, and Future of Refugee Protection and Solutions: Camps, Comprehensive Plans, and Cyber-Communities." Emory International Law Review, vol. 31, no. 4, Oct. 2017, pp. 539–552. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=125053370&site=eds-live.

Armerding, Taylor. "The 18 Biggest Data Breaches of the 21st Century." *CSO Online*, CSO, 20 Dec. 2018, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Bell, Cameron H. "Cyber Warfare and International Law: The Need for Clarity." *Towson University Journal of International Affairs*, vol. 51, no. 2, Spring 2018, pp. 21–42. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=poh&AN=130308863&site=eds-live.

Broad, William J., et al. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times*, The New York Times, 15 Jan. 2011, www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

California Department of Insurance. "Investigation of Anthem Cyber Breach". 6 Jan. 2017.

Carr, Jeffrey. "In Tunisia, Cyberwar Precedes Revolution." *Forbes*, Forbes Magazine, 15 Jan. 2011, www.forbes.com/sites/jeffreycarr/2011/01/15/in-tunisia-cyberwar-precedes-revolution/#8c884894604c.

Clarke, Rachel, and Taryn Youngstein. "Cyberattack on Britain's National Health Service — A Wake-up Call for Modern Medicine." *New England Journal of Medicine*, vol. 377, no. 5, 3 Aug. 2017, pp. 409–411., doi:10.1056/nejmp1706754.

Dankova, Petra, and Clotilde Giner. "Technology in Aid of Learning for Isolated Refugees." Forced Migration Review, vol. 1, no. 38, Oct. 2011, pp. 11–12. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=67299408&site=eds-live.

Delany, Colin. "How Social Media Accelerated Tunisia's Revolution: An Inside View." *Epolitics.com*, 24 Dec. 2017, www.epolitics.com/2011/02/10/how-social-media-accelerated-tunisias-revolution-an-inside-view/.

Field, Matthew. "WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled." *The Telegraph*, Telegraph Media Group, 11 Oct. 2018, www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

Gazula, Mohan B. "Cyber Warfare Conflict Analysis and Case Studies." *Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*, vol. 2017, no. 10, May 2017.

Gorman, Leta. "The Era of the Internet of Things: Can Product Liability Laws Keep Up?" *Defense Counsel Journal*, July 2017.

GSMA. *The Importance of Mobile for Refugees: A Landscape of New Services and Approaches*. GSMA, January 2017.

Harwell, Drew, and Ellen Nakashima. "China Suspected in Major Hacking of Health Insurer." *The Washington Post*, WP Company, 5 Feb. 2015, www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html.

Hopping, Clare, and Dale Walker. "NHS Ransomware: UK Government Says It's North Korea's Fault WannaCry Happened." *IT Pro*, 20 Dec. 2017, www.itpro.co.uk/security/28648/nhs-ransomware-attack.

"Jesuit Commons: Higher Education at the Margins (JC:HEM)." *Center for Education Innovations*, 15 June 2015, educationinnovations.org/program/jesuit-commons-higher-education-margins-jchem.

JRS USA, www.jrsusa.org/.

Kerner, Sean Michael. "WannaCry Ransomware Attack Hits Victims With Microsoft SMB Exploit." *EWeek*, May 2017, p. 1. *EBSCOhost*, login.avoserv2.library.fordham.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=123052453&site=eds-live.

Knopová, Martina, and Eva Knopová. "The Third World War? In The Cyberspace. Cyber Warfare in the Middle East." *Acta Informatica Pragensia*, vol. 3, no. 1, 2014, pp. 23–32., doi:10.18267/j.aip.33.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum: Technology, Engineering, and Science News*, 26 Feb. 2013, spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

"Major Ransomware Attack Sweeps Europe." *Pindrop*, 8 Sept. 2017, www.pindrop.com/blog/uk-hospitals-hit-by-broad-cyberattack/.

Manzo, Vincent. "Stuxnet and the Dangers of Cyberwar." *The National Interest*, The Center for the National Interest, 29 Jan. 2013, nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030.

Mathews, Anna Wilde, and Danny Yadron. “Health Insurer Anthem Hit by Hackers.” *The Wall Street Journal*, Dow Jones & Company, 5 Feb. 2015, www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

“National Centres of Competence in Research (NCCRs).” *SNF*, www.snf.ch/en/researchinFocus/nccr/Pages/default.aspx#Completed%20NCCR.

Spini, Dario, et al. “Vulnerability across the Life Course: A Theoretical Framework and Research Directions.” *LIVES Working Papers*, vol. 2013, no. 27, 2013, pp. 1–35., doi:10.12682/lives.2296-1658.2013.27.

Sprusansky, Dale. “From Blogs to the Street: Juan Cole Discusses Tunisia’s Youth Activists.” *Washington Report on Middle East Affairs*, no. 8, 2014, p. 64. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edsggo&AN=edsgcl.393656713&site=eds-live.

States News Service. "Tunisia: End use of Excessive Force; Free Political Prisoners". *States News Service*, January 14, 2011 Friday. https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:51Y9-4YX1-DYTH-G2TX-00000-00&context=1516831.

Symantec Security Response Team. “What You Need to Know about the WannaCry Ransomware.” *Symantec*, 23 May 2017, www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

Talihärm, Anna-Maria. “Towards Cyberpeace: Managing Cyberwar Through International Cooperation.” United Nations, www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

Talukder, Asoke K., and L. M. Patnaik. *Innovative Applications Of Information Technology For The Developing World - Proceedings Of The 3rd Asian Applied Computing Conference (Aacc 2005)*. Imperial College Press, 2007. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=516741&site=eds-live.

Tschider, Charlotte A. “Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age.” Denver Law Review, vol. 96, no. 1, Nov. 2018, pp. 87–143. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=135154524&site=eds-live.

United Kingdom, National Audit Office, Sir Amyas Morse KCB. “Investigation: WannaCry cyber attack and the NHS”. 24 Oct. 2017.

United Nations. *World Economic Situation and Prospects*. United Nations, 2019.

Williams, Patricia AH, and Andrew J. Woodward. "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem." *Medical Devices: Evidence and Research*, 8 (2015): 305-16.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, Conde Nast, 3 June 2017, www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.