Thesis Portfolio

CS XXXX: Cybersecurity in the Cloud
(Technical Report)

Engineering's Commitment to the Public Welfare
(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering and Applied Science

Justin Hoon Kim

Spring, 2021

Table of Contents

Sociotechnical Synthesis

As technology becomes more advanced and pressures more systems to move to the cloud, there arises a question of how engineers can maintain security and privacy. However, even before the engineering community can begin to answer, a deeper and more alarming issue within American society must first be addressed. An increasing number of engineers are becoming unconvinced that they owe any significant responsibility to the public welfare.

For my capstone project, I attempt to contribute to the engineering community by educating computer engineers on current cybersecurity capabilities in the cloud. My team and I created a partial curriculum for a university course. We aggregated information that we gathered from previous classes, researched additional security methodology, and focused our class material on specialized security for the cloud. By the end of the project, we were able to deliver a syllabus outlining the weekly curriculum for the course and a sample of the first four weeks. The objective for each week is that students would be able to understand a new cloud security subject and be capable of implementing a related, secure practice in any outside projects. We showed the curriculum to other students and received an overwhelmingly positive response. As a result, we are convinced this course would benefit not only UVA engineers, but by extension, the engineering community as a whole.

For my sociotechnical research, I attempt to address the underlying issue of the culture of disengagement in the United States. My research comprised of examining the factors that have led to engineers neglecting their ethical responsibilities and possible solutions to reverse this effect. I use Project Raven as a case study to tangibly understand this culture, both its elements and its ramifications, and how my suggestions could have prevented these outcomes. The most important results from this research were the actions that the engineering community can take

both academically and professionally to inculcate and promote a commitment to the public welfare among engineers.

I believe the work I contributed is valuable to the engineering community. I was able to create an outline for a class that would not only be beneficial to students, but also included solutions from my STS research to instill a stronger commitment to the public welfare. My sociotechnical research is very fruitful to society as it suggests methods to promote ethics in engineering, a field that is very apparently deteriorating. The biggest adversity through this process was the frustrations of COVID and having a lack of face-to-face interactions. For future researchers, I would recommend continuing to develop the curriculum my team started as well as implementing the suggestions in my sociotechnical research to have tangible results.

I, first and foremost, thank my God for blessing me with the opportunities to attend and succeed at UVA. I would also like to thank my family and friends who have supported me through my journey. Lastly, I would like to thank my professors, specifically Professors Sean Ferguson and Aaron Bloomfield, who were significantly instrumental in my research.

CS XXXX: Cybersecurity in the Cloud

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Justin Hoon Kim

Spring, 2021

Technical Project Team Members
Justin Hoon Kim
John Light
Ranjodh Sandhu
Karanvir Jassal

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Justin Hoon Kim

Approved _____ Date _____
Advisor Name, Department of Computer Science

Abstract

In an age where speed and efficiency have been the primary measures for progress, there has been a mass migration of information and processes to online platforms, specifically the cloud. As such, there are those who seek to exploit this shift in medium, attacking cyber structures and frameworks within the cloud, for their own private gain. With each iteration of vulnerabilities and patches, attacks are only becoming more ingenious and harder to detect. Thus, it is no secret that traditional cybersecurity practices have not been able to keep up with the pace of growth in the cloud.

While schools have attempted to teach students these traditional practices as foundational in their own local projects, little effort has been made to apply them to the cloud computing environment. Introductory cybersecurity courses tend to focus more on understanding the basics of advanced topics in cybersecurity including encryption, digital forensics, binary exploits, and networks. These naturally tend to be more focused on programming against certain attacks. While that is appropriate in its own regard, with cloud environments, many of the security components are based on configuration. A user does not need to code the solution but use the available tools and resources to best secure the system in its particular use case. This is crucial as oftentimes, entire processes run on the cloud so there is a lot at stake when working on cloud platforms.

In order to bridge this gap, we propose a class that incorporates aspects from two different computer science courses at the University of Virginia -- CS 3710: Introduction to Cybersecurity and CS 4740: Cloud Computing. To develop this new class, we examined the documentation for these courses and expanded on their overlap. As former students of these courses, we reflected on their strengths and weaknesses in order to improve the structure of the new class and provide an experience that is tailored to cloud computing. As a result, students will better understand threats to the cloud structure and learn the safe practices that will help mitigate the associated risks. They will also be better equipped to handle cybersecurity issues when working in the cloud for their future careers, creating a safer and more secure environment for their clients and stakeholders.

While the class will have a focus on cybersecurity in the cloud environment, it will also aim to highlight some of the growing topics within cloud computing. Two growing fields that have had much controversy around them are Artificial Intelligence and the Internet of Things. While these two technologies have a tremendous amount of potential, they also pose some security concerns for users that have held them back. This course would allow students to explore some applications of these technologies while also educating students on how to develop solutions in an ethical and secure manner. Both the Internet of Things and Artificial Intelligence are data-driven and many people do not have confidence that the data they are using is secure and collected ethically. So this course will aim to highlight practices that can keep the data in the hands of those that are meant to see it and how to gather data in ways that gain trust of the users. A student who has finished this course should be able to understand the concerns of users while developing solutions in the cloud environment. The generalized overview that CS 3710 and 4740 both bring is valuable so this course is not designed to replace them. Instead, this course is designed to be taken

after completing CS 4740 because it will be more specialized.

During the first two weeks there will be a big review period of basic cloud terminology and essentials that were taught in 4740 and also a review on the class 3710. This will also go over new topics such as user and group permissions, authentication issues, and also cloud security basics. Then the next few weeks will be about network security revolving around the cloud including network addressing, network protocol layers, and network devices. This will give the student a better understanding of how different hosts interact within a network. Then the next several weeks will focus on Public-Key Crypto, Hashing for Authentication, Network Authentication, Authenticating Network Servers, Digital Signatures. Then the course will end on introducing more miscellaneous topics including how artificial intelligence and the internet of things are kept secure and good practices when it comes to security when dealing with those spectrums.

Introduction

Cloud computing is one of the fastest growing areas of computer science, and there needs to be more than one class available on the subject. Cyber security is important everywhere there is computer science, and this class helps students see where it's applied in the cloud. Currently, in order to get an understanding of cyber security, students need to take CS 3710 for an introduction, and also CS 4630 Defense Against the Dark Arts (DADA). Our class aims to dig deeper into cyber security, similar to 4630, but with a specific focus on the cloud. This way, instead of taking a generalized cybersecurity course, if students and particularly interested in cloud computing, they now have an option. The four of us have all taken CS 3710 and 4740, and three of us have taken 4630. When deciding what kind of class we wanted to create, the overlap between the courses had a lot of potential information we thought could be interesting to learn.

With many companies transitioning either completely or partially into the cloud, many companies have an increased reliance on the cloud. Cloud services are supporting entire operations and even contain sensitive information. With the shared responsibility model in the cloud, it is important that all users follow secure practices when operating in the cloud. This can help companies save resources and keep their information safe. As the liability can fall on the consumer rather than the provider, we believe that focusing on fundamentals will enable students to be successful in their careers. The experience and knowledge that students gain from this course will impact how they interact with the cloud.

Background

To understand the need for this course, one needs to know the course offerings for computer science at UVA. There is currently no class that covers this material, though there exist the ones mentioned above that are related. However, they don't go into the specifics of cybersecurity in cloud computing.

CS 4740 provides an introduction to cloud computing as it consists of a general overview, but since cloud computing encompasses so many different services, it is not possible to go in depth. Currently, if a student takes that course and decides that they are interested in pursuing a career in cloud computing, they don't have many course options. A focus on security in the cloud will enable students to begin going more in-depth with cloud computing. We believe that this course is the first cloud

computing course that should be taken after CS 4740 because of the complexity of vulnerabilities that can arise in the cloud environment. Before advancing into the different realms that exist within cloud computing, it is important that students have a solid foundation of this topic that is relevant everywhere in the cloud. Whether a student decides to focus more on artificial intelligence or cloud storage, they must first know how to secure the data and resources that they are working with.

While CS 3710 is an introduction to cybersecurity, the aim of this class is to show students how specifically the cloud environment is vulnerable to attacks. CS 3710 gives students a very broad idea of security but does not cover any attacks such as SQL injection attacks, cryptography, and network security as it relates to specifically cloud computing. Furthermore, this is becoming a more and more relevant field as more and more companies are moving towards cloud computing and adopting it. This will create a need for cloud security experts that can prevent hackers from exploiting companies' data.

Related Work

When looking up information for this course, we saw that other universities had courses that covered what we wanted to cover, reassuring us that this need does exist and that adding this class would be beneficial for UVA.

System Design

Our project was designed with the goal of taking information from two courses, CS 3710 and 4740, and digging deeper into their overlap. This class is for people who have an interest in cybersecurity and how it applies to cloud computing. The objectives of this class are for students to learn about threats to the cloud structure and learn the safe practices that will help mitigate the associated risks, understand how to handle cybersecurity issues when working in the cloud for their future careers, creating a safer and more secure environment for their clients and stakeholders, and explore the applications of IoT and AI while developing solutions in an ethical and secure manner. Our course design was a 16 week class with weekly quizzes, homeworks, and one final exam: The assignments are worth 60% of the grade, tests 20%, and quizzes 20%. We believe that the best learning takes place when students are applying the concepts. We wanted our grading structure to reflect a structure that promotes learning over the pressure of doing well on an examination.

Week 1 reviews the syllabus and touches on some concepts from 3710/4740. Week 2 and 3 go over some cloud data security information. Week 4 goes over session management and application security. In our final submission, these are the four weeks we created powerpoint lectures, quizzes, and assignments for. We split up our powerpoints so there would be two lectures per week. In the last 12 weeks, week 5-7 go over cryptography, network controls, and providers/scripts respectively. Weeks 8 and 9 go into detail about attacks like SQL injection and cloud based attacks. Weeks 10 and 11 talk about how to manage vulnerabilities and protect your data. Weeks 12-16 aren’t specific about cybersecurity and the cloud, but discuss two other important topics in artificial intelligence (AI) and Internet of Things (IoT). These last two topics give students the opportunity to apply the knowledge they have gained throughout the semester in a fun way. AI and IoT are two technologies that have been growing rapidly and are major use cases for the Cloud. Working with these technologies is a way of rewarding the students at the end of the semester as they get to develop in the

cloud while also making sure they are being safe and secure. Similar to current CS courses, lectures are recorded and available to listen to outside of class. Most homework assignments will require students to use AWS, some scripts, and Python to complete. To align with UVA honor code policy, this course's honor code is also single sanction; if you are caught cheating, you will fail.

We decided that, for each week, it was important to include lecture material through the form of a powerpoint, a homework assignment, and a weekly quiz. We thought that all of these materials combined would qualify for enough classwork and would amount to the proper number of credit hours for a three credit course. Additionally, other classes we have taken generally assign a similar amount and type of work per week. The students would be able to learn and receive information from the powerpoints. The instructor would ideally lecture based on the slides. To test the students' learning and mastery over the week's material, a weekly quiz is designed to ensure each student took away the most important elements of the week's lesson. The quizzes would be open notes, since the purpose of the class is not to rank students based on grades and performance but to confirm that they are learning the material. If it seems that students are performing poorly on the quizzes, supplementary activities should be provided or additional office hours should be held. Finally, the assignments are to allow students to practically apply their educational knowledge. In our college experience, we have found that homeworks and assignments are the most vital piece of education for learning and information retention. The practice not only gives students the chance to experience potential real world applications, but the act of applying knowledge to an assignment also forces students to actually understand the material. Thus, we designed each week to comprise these activities.

For Week 1, we wanted to ease into the transition of classes and do what most classes do during week one. Essentially, we thought it would be beneficial to the students to go over the syllabus, what topics we will be covering during the class, honor policy, and expectations. Going through this information first is very important as students can get a feel of what the class will behave like and what the workload will consist of. Furthermore, a requirement to continue the class will be for students to sign the syllabus and return it which will also contain the agreement to uphold the honor system. Also in the first week, there will be an emphasis on logistics and how the class will be run. This will include introducing the TA's and their office hours. After all the class information is taken care of, the class will start diving into a basic review of Cloud Computing and Security. Firstly, the review will start with This will include covering topics such as PaaS, IaaS, and SaaS and discussing the main differences between the three services. After that, the content for the week will shift focus on the security basics. This will include a rundown of some common techniques used to exploit vulnerabilities and data such as phishing, distributed denial-of-service (DDoS) attack, and a brute force attack. The assignment will then focus on the students writing a python script and using a password cracking (brute force) technique. Along with that coding assignment there will be an essay due that will have the students research about past incidents of where these attacks have actually occurred and used to steal data from tech companies.

For Week 2, we thought that it would be best to focus on cloud data security, which consisted of privacy and protecting data. Since this would only be the second week of

classes and students may still be adjusting their schedules, beginning with these concepts would be a good way to ease students into the more complex topics. The first topic introduced in this week is protecting data. We decided to focus on the different types of data that exist and how they can be protected. Many clients and companies use the cloud for data storage so it is important to be able to distinguish the information that exists in each type and how it can be secured. In addition, this course highlights the importance of keeping company and data secure by going through some examples of fraud throughout history. After that, the content for the week focuses on privacy laws and external regulations for specific sectors. After learning the different concepts relevant to the week's topics, the assignment aims to help students apply those same concepts in the cloud environment. Since we believe that the best way to learn is by doing, we get students to sign up for AWS during the second week of the course so that they can dive in early on. After signing up, the students are tasked with securing an S3 bucket to limit access to specific users that they select. The goal of this assignment is to have students create a mindset of limiting access to only those who need it across all services. This week emphasizes the importance of understanding the domain of the work being done. Computer science, as a whole, has the potential to impact many different fields from medicine to business. This, however, means that as someone working with these different areas, an engineer must be aware of the expectations of those domains as well. Talking about external regulations and privacy laws helps establish that while standards exist across different fields, the depth and extent of the privacy and security varies. It is not a "one size fits all" approach when it comes to privacy.

For Week 3, we wanted to transition from understanding cloud data security and its broad practices to practical and specific implementations of cybersecurity in the cloud. The first and most common practice is Identity Access Management, or IAM. Naturally, we decided to focus on this specific subject matter first. Given the vast topic of IAM, we thought it would be sufficient enough to cover a week-worth of material. The overall objective of this week was to help students become familiar with IAM, understand identities and permissions for AWS resources, and be capable of maintaining a secure AWS environment. Thus, by the end of this week, students should be able to set up and configure users, groups, and roles; implement multi factor authentication; create IAM policies; implement password policies for security controls; and understand the AWS Key Management Service. Looking at the information concerning IAM, we decided we could break it down into six sections to make it more digestible for students. The first section is the overall background of IAM -- defining IAM itself, its purpose, and any terms that are commonly seen when dealing with IAM. Next, students would learn arguably the most important part of IAM, creating the actual objects that would be given or restricted access. During this portion, students would learn how to create and manage users, groups, and roles and understand the nuances between each object. Once students have a concrete understanding of creating objects, the curriculum focuses on the creation and customization of IAM policies themselves. Then, the students would have time to learn about additional AWS security features associated with IAM such as multi factor authentication, identity federation, and other miscellaneous security techniques. This material is supplemented by a quiz that has a mix of recall and application. We thought

the couple recall questions included on this quiz were based on facts that any computer science student dealing with cloud and security ought to remember at all times. Overall, the intent of the quiz was to make sure that each student thoroughly understands each of the objectives for the week. Finally, there is a homework assignment attached with this week's curriculum. The assignment is designed to guide students to be able to create users, groups, and policies and attach permissions to these objects, essentially using the lectures to be able to implement IAM. Thus, through the powerpoint, quiz, and assignment, we decided that these would best teach students on how to properly implement and use AWS IAM and why this is important.

In Week 4, we thought that after exploring the cloud the previous two weeks, that it would be a good time to introduce some basic application security and session management to begin incorporating cybersecurity information. We start by discussing an important clarification between authentication and authorization as a background for session management, which is discussed in the second lecture this week. After clarifying the difference, we talk about ten common security risks for applications, and go into further detail about two of them: Cross site scripting and SQL injection attacks. In the classes we've taken, we felt like doing these attacks as homework really helped our understanding; we hope that the homework assignment for this week, which is an XSS and SQL injection attack on a practice website, would be beneficial. In the second lecture, we go over session management, the importance of session IDs, and the roles that cookies play in session management. With week 2 and 3 providing the groundwork for cloud computing, this week aims to lay the foundation for cybersecurity. To end the week, we have a quiz that tests the students' understanding of authentication vs. authorization, common attacks and how to defend against them, key aspects of session management, and SQL/XSS attacks.

Results

After showing this course to several students that have previously taken at least one of the two courses (CS 3710 or CS 4740), we have gotten some promising results. A survey was conducted to see if this course was effective in teaching security in cloud computing given the four weeks of material to 5 students, and these are the results. There were four main questions that were asked after the students reviewed the material from the four weeks and looked at the quizzes and assignments.

The questions consisted of:

How much of the information did you already know? (1-5)

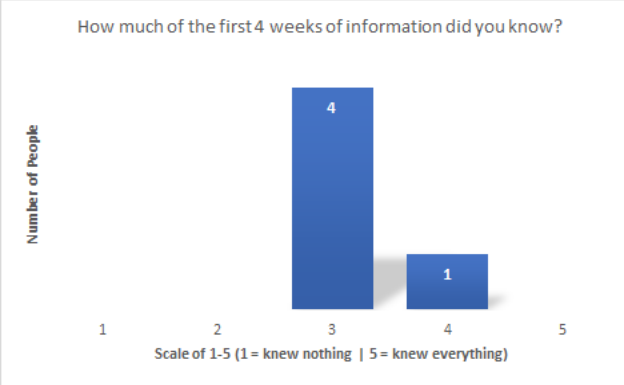
Do you think this course would help you gain knowledge in security relating to cloud computing? (1-5)

How interesting are the topics that are covered in the course? (1-5)

How likely are you to recommend a fellow student to take this course? (1-5)

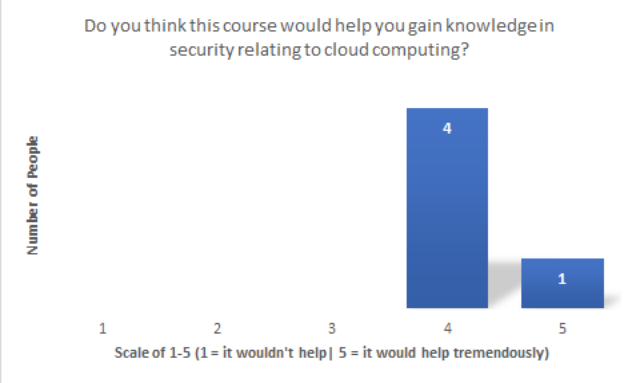
The graphs for the following questions are presented below:

Question: How much of the information did you already know? (1-5)



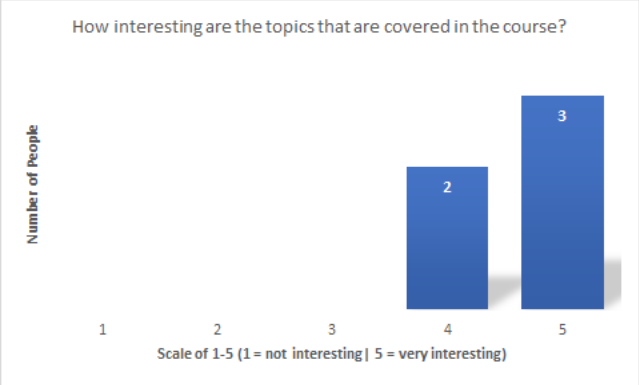
Most of the students said they knew some of the information, but not all of it. This shows us that while there is some overlap with the courses this class is inspired by, there is still new information that students haven't seen.

Question: Do you think this course would help you gain knowledge in security relating to cloud computing? (1-5)



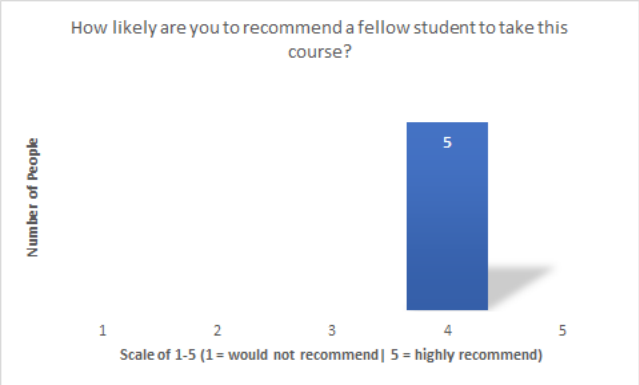
Most of the students rated that this course stated that this course would indeed help them learn about security measures relating to cloud computing, and said the structure of material was designed well.

Question: How interesting are the topics that are covered in the course? (1-5)



The response here was overwhelmingly positive, with comments about how cybersecurity is an interesting field and any more teachings on it are welcome.

Question: How likely are you to recommend a fellow student to take this course? (1-5)



The responses for this question were all the same. Our interpretation of why this was is because this class would be an upper level course, students here could potentially already be well versed in some of these topics, and it wouldn't make sense for them to take it. However, for people without that knowledge and that have an interest in these topics, it would make a lot of sense to take this course.

Conclusions

We designed a class to address the need for expanded information where CS 3710 and CS 4740 overlap. Our course begins with a review of concepts from those two courses, then goes into detail about cyber attacks and

defenses in the cloud, and ending with a discussion of AI and IoT. Students are tested weekly through quizzes and homework assignments, ending with a final exam. We believe that this course is necessary, as similar courses exist in other universities, and that it will provide a more comprehensive understanding of cloud computing and cybersecurity. This course will provide students with valuable information that they will be using when they enter the workforce, given that the role uses cloud computing services. Many people and companies have critical data stored on the cloud and any misconfiguration can be exploited. With the shared responsibility model that exists with cloud computing services, the liability of keeping the data secure on a digital level is in the hands of the user.

Before focusing on any specific area of cloud computing, it is important that students have a solid foundation on a topic that is prevalent everywhere in the cloud. By providing students with this fundamental skill and mindset, this course will enable students to use cloud services safely in future courses or work. The course also touches on ethics as cloud computing can be data-driven. This is done with the hopes that students will understand how to work ethically and within the regulations that exist within different fields of work. Working with cloud services may entail handling data from other sectors such as medical or financial. By having a better understanding of regulations and laws through this course, students will understand the security expectations when handling different types of data and have a better idea of how to proceed with the information.

Future Work

Currently, this project consists of a general overview of the course as well as material for the first 4 weeks of classes. These materials include a slide deck, a take-home assignment, and a quiz. If this course were to be implemented at the University of Virginia, the materials for the rest of the weeks would need to be developed as well as an examination. In addition, the first couple of semesters of this course's offering would bring more information and feedback on how this course could be adjusted.

The main work that needs to be done in the future is flushing out the assignments. Currently, the four weeks assignments are sufficient but creating the other 3-6 assignments for the other weeks will take some more creativity and time. Furthemore, we have not written any tests for this class as of right now and in the future that will need to be taken into consideration. Lastly, we are considering adding a big group project for this class that would help students realize the importance of teamwork in both cloud computing and security.

REFERENCES

[1] Amazon. (2003). *IAM User Guide*. Amazon. https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.

[2] Amazon. (2003). *IAM*. Amazon. https://aws.amazon.com/iam/.

[3] Amazon. (2011). *Amazon Rekognition Developer Guide*. Amazon. https://docs.aws.amazon.com/rekognition/latest/dg/setting-up.html.

[4] *HIPAA Security Series*. U.S. Department of Health & Human Services. (n.d.). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf?language=es.

[5] *OWASP Top Ten*. OWASP. (n.d.). https://owasp.org/www-project-top-ten/.

[6] *PCI DSS Quick Reference Guide*. PCI Security Standards. (n.d.). https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

[7] *Session Management Cheat Sheet*. Session Management - OWASP Cheat Sheet Series. (n.d.). https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html.

[8] Tierney, M. (2020, July 2). *Data Security in Cloud Computing: Key Components*. Netwrix. https://blog.netwrix.com/2020/07/02/cloud-data-security/.

[9] *What Is Cloud Data Protection?* Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection#:~:text=Cloud%20data%20protection%20is%20the,externally%20by%20a%20third%20party.

[10] YouTube. (2017, December 4). *AWS IAM | AWS IAM MFA | How to Create User, Group, Role,Policy and MFA*. YouTube. https://www.youtube.com/watch?v=Ihpkf3xwuJo.

Engineering's Commitment to the Public Welfare

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Justin Hoon Kim

Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Justin Hoon Kim

Approved _____ Date _____
Sean Ferguson, Department of Engineering and Society

Engineering's Commitment to the Public Welfare

Engineers are among the primary influencers of society. Their contributions and technologies so impact the culture around them that they innately, regardless of intention, shape modern institutions and affect future directions. Thus, while progress and advancement are noble causes, it is of upmost importance for engineers to be guided primarily by a set of ethical standards, specifically framed around the commitment to public welfare. As such, engineers ought to manifest their ethical responsibilities, understand the potential usage and consequences of their technologies, and develop a strong social cognizance.

There has, however, been engendered a culture of disengagement within the modern engineering community (Cech, 2014). Due to the lack of cultural emphasis on the aforementioned obligations, many engineers have fallen away from their commitment to the public welfare. They do not thoroughly question the morality of their actions and ignore the ethical ramifications of their technologies. More and more, engineers are both treated like and act as blind tools for an end rather than ethically cognizant human beings (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). As such, they have become increasingly unaware of their power to vastly shape sociotechnical systems and have, thereby, unintentionally exacerbated issues such as privacy; control, influence, and power; international relations; and human rights violations. Thus, this paper will attempt to examine the factors that have led many engineers to disregard their commitment to the public welfare and how society can re-instill those values within engineers. Project Raven will be used as a case study to exemplify this issue and suggest common solutions to create principled engineers.

Commitment to Public Welfare and the Culture of Disengagement

Although ethics and science are two separate fields, they ought to be inextricable. As technology is the material facts that guides progress and advances society, ethics ought to be the nonmaterial beliefs that guide technology (Graham, 1982). So, for a society that values and grounds its ethics in efficiency and equity, its individuals and structures must work to maximize utility for all of society's participants, or increase the public welfare.

Public welfare is mainly concerned with social justice, equity and equality, risks and benefits, and the rights of privacy, monitoring, and control. For the engineer, public welfare describes how his or her work influences the general public, either positively or negatively (Kulacki, 1999). There will, however, be difficulties in accurately determining this influence because of the principle of double effect, or the idea that most actions will have more than one effect. While engineers' primary intentions must be aimed at virtue and good, never seeking immoral results and striving to avoid being complicit in evil, there will be unintended and unavoidable consequences to any moral actions (McIntyre, 2019). Hence, when developing new technologies, engineers must be ethically cognizant of how their designs might cause injustices to direct and indirect stakeholders (Friedman, 1996). It is under the commitment to the public welfare that engineers ought to constantly consider their impact to the general public.

Culture of disengagement is how engineers think, design, produce, talk about and evaluate their work. Engineers determine elements that are necessary to their design responsibilities and "what concerns they can bracket" (Cech, 2014). Through this process, commitment to public welfare is normally defined out of the scope of an engineer's responsibility as they are not "directly relevant to the design or implementation of technological objects and systems" (Cech, 2014). Thus, culture and disengagement can be summarized in three pillars: (1) depoliticization, the idea that technology ought to dissociate with social concerns for

fear they may corrupt the design process; (2) technical/social dualism, the idea that the most valued technical works are those that "allow engineers to bracket social consideration most extensively"; and (3) meritocracy, the idea that social structures in the United States are just as it places people in social groups based on merit and hard work (Cech, 2014).

Unfortunately, there has been a shift away from commitment to public welfare and towards a culture of disengagement in the United States. While simple ignorance, shallow understanding of loyalty, or absence of oversight do compound to this shift, the lack of education and training is largely responsible for fostering such a culture (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). Consequently, the United States risks falling into the same pattern as the Soviet Union and modern-day Russia. Andrei Soldatov, an investigative journalist and Russian security services expert, describes this environment:

> The Soviet Union many years ago, enjoyed the largest engineering community in the world. Stalin launched lots of so-called polytechnical schools because he needed lots of engineers to help him build the mighty military-industrial complex. But, a specific thing about the Russian technical education, still, is that in these schools you are not taught ethics. The idea is that an engineer should just provide technical expertise. Never ask any questions. When the Soviet Union collapsed, they ended up in some computer companies. So, we have lots of these people who are quite ready to help the government if the government wants them to do something. And we have lots of people who started doing stuff because they have technical skills, but they have no ethics at all (Soldatov, 2018).

Soldatov theorizes that an education that produces capable and excellent engineers with no ethical background will inherently create a culture that promotes technical and scientific advancement simply on the basis of ability, that people will do things just because they can. Additionally, he attributes the 2016 United States election hacking scandal to this mentality. The Russian engineers were used as tools to an end and blindly trusted the government for their ethical guidelines; they had not been trained to create their own moral compass and so could not ask questions of morality (Soldatov, 2018).

And it is the preconditions for this environment that the United States is establishing. According to Niles et al. (2020), “increasing engineering students' engagement with public welfare is central to promoting ethical responsibility among engineers and enhancing engineers' capacity to serve the public good”. However, while it is evident that engineers’ ethical thinking and behavior must begin within their education, research by Erin A. Cech determined that, in the United States, “students’ interest in public welfare concerns may actually decline over the course of their engineering education” (Cech, 2014). Examining four different American universities, specifically MIT, University of Massachusetts Amherst, Olin, and Smith, researchers found “students’ beliefs in the importance of professional and ethical responsibilities, understanding the consequences of technology, understanding how people use machines, and social consciousness all declined” (Cech, 2014). As can be seen in Figure 1, in each of these categories, there was statistically significant evidence that the decline was due not to chance but the education the students had received. Furthermore, there resulted a direct relationship between the emphasis of public welfare engagement within the university curriculum and the students’ public welfare beliefs. Students who reported that their school did not emphasize engagement were found to have lower public welfare beliefs than those who reported more cultural emphasis, and vice versa. Thus, although there is hope that general education and cultural emphasis can instill strong public welfare beliefs within engineers, it was concluded that these beliefs are not valued enough in engineering circles (Cech, 2014).

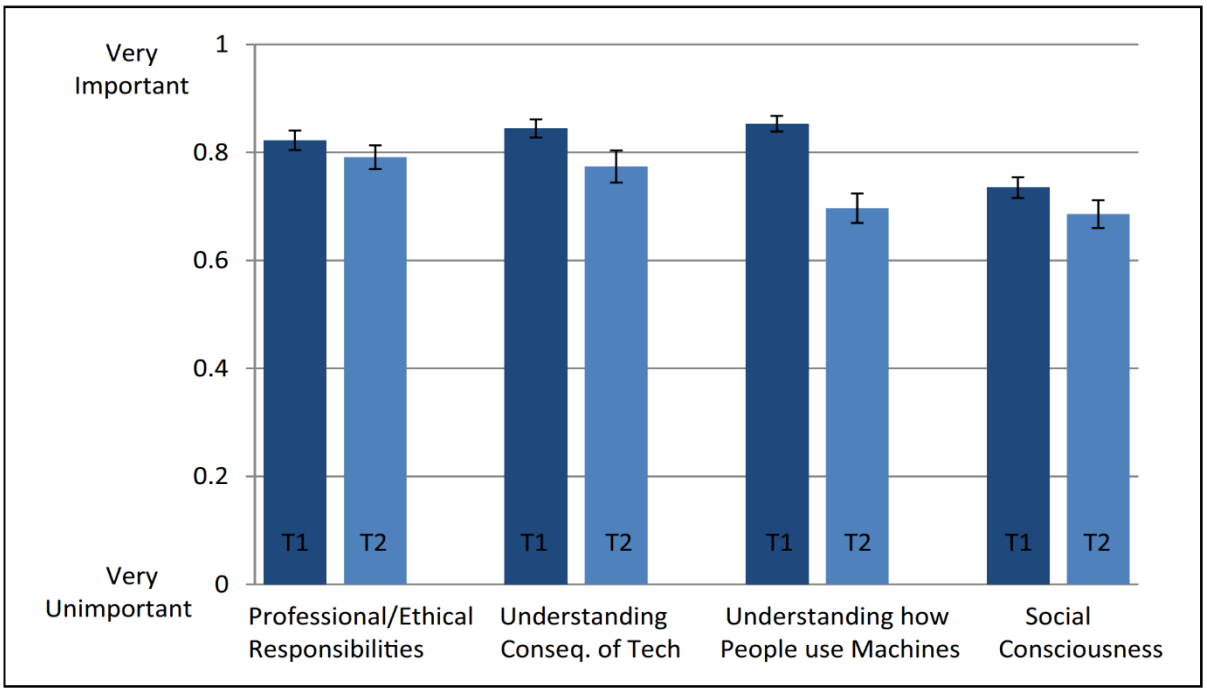


Figure 1: Public welfare beliefs among engineering students, time 1 and time 2. Dark bars represent the mean value on that measure at time 1 and the lighter bars represent the mean value on that measure at time 2 (Cech, 2014).

To many of the universities' credit, Cech did recognize that many higher education programs had started to shift focus on creating a culture that places more emphasis on public welfare. However, there were many difficulties and obstacles in doing so (Cech, 2014). The Journal for Engineering Education attempted to explore this phenomenon, specifically by naming the "challenges facing efforts to increase engineering students' engagement with the social and ethical implications of their work" (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). They categorized the challenges into four main areas:

> (a) defining and defending their identities as engineers; (b) justifying the value of nontechnical work and relevance to engineering; (c) redefining engineering expertise and integrating community knowledge into projects; and (d) addressing ambiguous questions and ethics (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020).

In defining and defending identities, it was found that students were stigmatized into feeling that engaging with public welfare was neither a legitimate aspect of "real engineering"

nor a part of their identities as engineers. They expressed the difficulties in navigating through the technical/social dualism and constantly defending that engineering extends past solely the technical lens. Then, if the students were able to successfully define and defend their identities as engineers, they often had issues justifying the value of nontechnical work and relevance to engineering. While they were able to understand the importance of the public welfare, "their embrace of nontechnical work was often fraught and incomplete" as they continued to marginalize nontechnical, interdisciplinary, and community knowledge and practices (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). The students, themselves, fell into the identity that they had sought to change. Similar to this challenge was found the obstacle of redefining engineering expertise and integrating community knowledge into projects. While redefinition is important to expand the perspective of engineers, researchers found this process to be the one most wrought with tension. Students consistently resisted integrating new ways of thinking and valuing community knowledge, expressing frustrations and doubts when they found the Western scientific method often incompatible with community knowledge. Finally, the last area of conflict was in addressing ambiguous questions and ethics. Since ethical questions often do not have definite answers, addressing these issues proved to be difficult to engineering students whose typical focus is on measurable constraints and clear solutions. Thus, these compounding challenges within the academic setting have contributed to the shift from a commitment to the public welfare to cultures of disengagement among engineers within the United States (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020).

Project Raven: A Case Study

As the culture of disengagement continues to grow in the United States, there is special concern in the field of computer science. The term "cyber-mercenaries" has emerged and is

becoming widespread (Nakashima, 2012). Private firms such as DarkMatter, NSO, Psy-Group, and Black Cube have begun competing to "lure top hacking talent from Israel, the United States, and other countries" (Mazzetti, Goldman, Bergman, & Perlroth, 2019). They understand the appeal to engineers who will be able to put their technical expertise to new use while being paid hundreds of thousands per year (Goldman, 2019). Compounded with a culture of disengagement, these engineers will become less concerned of their impact to the public welfare, making them the perfect tools for immoral ends. This paper will examine Project Raven, an exemplar case of the active manifestation of a culture of disengagement within the engineering community in the United States.

In 2012, a US-based government contractor, Cyber Point, entered into a contract with the newly established United Arab Emirates intelligence agency with the intention of giving advice on cybersecurity and policy. The ultimate goal of this project, Project Raven, was for Americans to "develop and run the program for five to 10 years until Emirati intelligence officers were skilled enough to take over" (Bing & Schetman, 2019). Thus, throughout the next few years, Cyber Point hired over a dozen ex-NSA operatives to work on the project. The offer was very appealing: perform essentially the same job as the NSA but with much more lucrative pay. All the information that was provided was that they would be fighting ISIS and would be tasked with hacking and collecting data on the UAE's enemies. They "would use methods learned from a decade in the U.S intelligence community to help the UAE hack into the phones and computers of its enemies" (Bing & Schetman, 2019). According to Lara Stroud, an operative on Project Raven, "The language and secrecy of the briefings closely mirrored her experience at the NSA giving her a level of comfort" (Bing & Schetman, 2019). In 2015, the UAE became uncomfortable with their intelligence being controlled by foreigners so they transferred the

project to a UAE backed contractor, DarkMatter (Mazzetti, Goldman, Bergman, & Perlroth, 2019). American operatives were given the option to transfer to DarkMatter or leave the project. The majority of chose to stay on the condition they did not spy on American citizens (Bing & Schetman, 2019). And although red flags did show up as spying on human rights activists and journalists became more prevalent, the general consensus was that the work "was incredible because there weren't these limitations like there was at the NSA. There wasn't … red tape" (Bing & Schetman, 2019). The engineers on the project were allowed to maximize their technical expertise without considering the ethical repercussions of their contributions. There no longer existed a structure that defined ethical boundaries for their work, and they were incapable of setting those boundaries themselves.

Thus, through Project Raven, one can examine how former US government employees so easily utilized their experiences, classified US surveillance techniques, and state-of-the-art espionage tools to spy on and censor human rights activists, journalists, and American citizens for foreign intelligence (Mazzetti, Goldman, Bergman, & Perlroth, 2019). The engineers on the project were too engaged in a culture of disengagement, one that was fostered even by the US government, that they were unable to think about morality until it was too late. Each pillar of disengagement existed in this case. Depoliticization was exemplified through the discouragement of questions and the fact that engineers were considered mindless tools that were expected to retire once they have exceeded their utility. The engineers refused to consider the ethical and social implications of their contributions as it might taint their work. They found their work to be exhilarating, not understanding the ethical purposes for the limitations imposed by previous employers (Bing & Schetman, 2019). Technical/social dualism was demonstrated by the operatives' feelings on Project Raven as a whole. They enjoyed the process and viewed ethical

boundaries as hindrances to advancement rather than essential considerations when designing technology (Bing & Schetman, 2019). Finally, meritocracy guided the decisions of many of the operatives. Human rights were secondary to work on the project itself. The social structures were just enough or at least subordinate to their advancements (Mazzetti, Goldman, Bergman, & Perlroth, 2019).

Lessons from Project Raven

What, then, can be learned from Project Raven? How can engineers be more ethically cognizant when developing technology, and how can society instill values of public welfare within them? Society needs engineers who are more willing to recognize and embrace sociotechnical complexities, whistle blow when they see immoral activity, and understand "how current practices of engineering problem definition and solution reproduce existing social inequalities" (Cech, 2014). They must be able to collaborate with and seek out advice from non-technical scientists, conceding some technical decision-making power and accepting non-engineering perspectives (Cech, 2014). Two solutions are apparent, one in the academic and one in the professional world.

The most immediate action that the engineering community can take is to inculcate public mindedness within students at engineering universities. This takes form in reframing college curriculums and experiences around engineering responsibilities that include public interest and public good (Kulacki, 1999) which starts with the incorporation of liberal arts into engineering education. According to Samuel Florman, a prominent engineer, "The liberal arts are what fill out a person's education, helping turn narrowly focused professionals into discerning citizens, intelligent communicators, and potential leaders" (Florman, 1996). However, not only do non-technical studies improve engineers' citizenships, but they also cultivate many morally

necessary technical and non-technical excellences such as techno-social sensitivity, respect for nature, and commitment to the public good. And, the liberal arts are able to do so by fostering sensibilities, emotions, and perceptions through history and literature. Stories are among the primary methods of developing virtues (Harris, 2008). Therefore, humanities and social sciences should not be on the peripheries of engineering education but ought to be incorporated within its foundations.

To further push commitments to public welfare in the academic setting, it is necessary for students "develop social networks and faculty support to both cope with frustrations and explore questions about public welfare engagement in more depth" (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). These networks allow students to process frustrations, share interests and excitement, and cultivate a sense of belonging within engineering. Additionally, research found that individual faculty played a significant role in increasing students' concerns for public welfare even at schools that did not emphasize this commitment in their curriculum. Conversations with faculty provoked greater interest and retention of engagement with public welfare concerns (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). Thus, not only do theses networks and relationships encourage discussions surrounding ethics but inherently engender a culture of engagement as thoughts on public welfare are normalized and prevalent in the engineering community.

Finally, in the academic world, individual classes ought to integrate technical education with learning about social contexts and impacts which has the additional benefit of making the classes engaging and relevant. "Engineering educators can centralize questions about social context and social inequalities into their classroom activities; can introduce a variety of epistemological methods in engineering, highlighting strengths, limitations, and assumptions of

each approach" (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). No longer would social ramifications be considered an afterthought, but students would be able to resolve the competing values within the technical/social dualism and understand engineering to be sociotechnical. This process would intrinsically couple the social context and public welfare with engineering, breaking down the preconditions of a culture of disengagement (Cech, 2014). Thus, by exposing students to social issues early in their education, society can more fully institutionalize a culture of engagement, broadening the perception of engineering and redefining what an engineer is.

While most of the solutions lie in the academic realm, there are necessary, immediate considerations to carry the culture of engagement to the professional world. First, employers of engineers must also understand the larger context of engineering practices and moral obligations that technical employees encounter (Kulacki, 1999). The aforementioned challenges for engineers become more difficult when their own employers try to indoctrinate a culture of disengagement by defining engineers' identities in the traditional sense (Niles, Contreras, Roudbari, Kaminsky, & Harrison, 2020). When engineers are expected to work without questions and are treated as tools for an end, it should not come as a surprise when they then begin to use their technical skills unethically. Instead, employers should offer resources to access ethical advice and tolerate actions engineers take in moral dilemmas (Goldman, 2019).

Second, employers ought to adopt an engineering ethics framework such as the Association for Computing Machinery's code of ethics. Using these outlines, employers can create more robust cyber ethics training programs that occurs at more frequent intervals, using case studies and creating likely scenarios that engineers may encounter. Especially in the context of the US government, engineers who are leaving after serving in cyber or intelligence ought to

also be given more than a "conflict of interest" training (Goldman, 2019). This can also take form of indoctrinating sociotechnical frameworks such as value sensitive design (VSD), the designing of technology that accounts for human values and direct and indirect stakeholders (Friedman, 1996).

If all of these solutions had been implemented in the case of Project Raven, it would have been difficult to imagine the rise of cyber-mercenaries. While it is hard to extrapolate that a more rounded education may have directly and ethically impacted the engineers on the project, it is clear that such an education would have, at the very least, provided a more solid virtuous foundation, one that would have questioned the morality of such a program (Nakashima, 2012). The engineers, then, may not have been opposed to all the guidelines and "red tape" they were required to follow (Bing & Schetman, 2019). Furthermore, had the US government and CyberPoint understood the larger societal context of engineering, they might not have trained engineers who were comfortable with and disposed towards secrecy. The engineers on the project would have been ethically cognizant of the ramifications of their contributions. Finally, the US government ought to have adopted a code of ethics and equipped engineers leaving their employment with tools on engaging with moral dilemmas (Goldman, 2019). Assuming that the engineers on Project Raven had used VSD to design their technologies, it is almost certain they would not have aided foreign nations in human rights violation (Friedman, 1996). Under the VSD framework, they would have identified the direct stakeholders as the UAE intelligence and ISIS terrorists. However, they would have also realized that their work indirectly affected private citizens, human rights activists, journalists, foreign nations, and citizens of other nations. If the UAE could use their technology to spy on ISIS, what prevented them from also using that technology to spy on anyone else with access to a virtual network? Thus, with a value system of

privacy, autonomy, human rights and social justice, and national loyalty, the US engineers on Project Raven could have easily determined that there were some moral repercussions of their work. Understanding that the project could potentially and unfairly discriminate against the more marginalized groups in society, in the very least, they would have been hesitant to join the project and their designs would have attempted to minimize bias using value-sensitive processes (Friedman, 1996).

Conclusion

It is without a doubt that engineers have significant influence in society. Thus, it is essential that engineers are trained to understand and take responsibility for the social implications of their technologies. However, today's society has only done the opposite. By ingraining depoliticization, technical/social dualism, and meritocracy, society has only managed to create a culture of disengagement. There is hope in reversing this effect and creating ethically cognizant engineers, though. By engaging at the academic and professional levels through the previously stated solutions, society can benefit their engineers and express the importance of the public good. How the future of social equity and justice looks depends on the inculcation of engineers today. Therefore, society must take on the responsibility to instill values and commitments to the public welfare.

References

Bielefeldt, A. R. (2018). Professional Social Responsibility in Engineering. In I. Muenstermann (Ed.), *Social Responsibility.* IntechOpen. doi:10.5772/intechopen.73785

Bing, C., & Schetman, J. (2019, January 30). *Inside the UAE's Secret Hacking Team of American Mercenaries*. Retrieved from Reuters: https://www.reuters.com/investigates/special-report/usa-spying-raven/

Cech, E. A. (2014). Culture of Disengagment in Engineering Education? *Science, Technology, & Human Values, 39*(1), 42-72. doi:10.1177/0162243913504305

Florman, S. (1996). *The introspective engineer.* New York: St. Martin's Press.

Friedman, B. (1996). Value-Sensitive Design. *Interactions*. Retrieved from https://cseweb.ucsd.edu/~goguen/courses/271/friedman96.pdf

Goldman, A. (2019, March 21). *Takeaways From The Times's Investigation Into Hackers for Hire*. Retrieved from The New York Times: https://www.nytimes.com/2019/03/21/us/politics/nso-darkmatter-government-spies.html

Graham, L. (1982). When Ideology and Controversy Collide: The Case of Soviet Science. *The Hastings Center Report, 12*(2), 26-32.

Harris, C. E. (2008). The Good Engineer: Giving Virtue its Due in Engineering Ethics. *Science and Engineering Ethics, 14*(153). doi:https://doi.org/10.1007/s11948-008-9068-3

Kulacki, F. A. (1999). Engineering, Engineers, and the Public Good. *William Mitchell Law Review*, 158-173.

Mazzetti, M., Goldman, A., Bergman, R., & Perlroth, N. (2019, March 21). *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*. Retrieved from New York Times: https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html/

McIntyre, A. (2019). Doctrine of Double Effect. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University. Retrieved from https://plato.stanford.edu/archives/spr2019/entries/double-effect/

Nakashima, E. (2012, November 22). *As cyberwarfare heats up, allies turn to U.S. companies for expertise*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html?noredirect=on&utm_term=.020886044ea2

Niles, S., Contreras, S., Roudbari, S., Kaminsky, J., & Harrison, J. L. (2020). Resisting and Assisting Engagement with Public Welfare in Engineering Education. *Journal of Engineering Education, 109*(3), 491-507. doi:https://doi-org.proxy01.its.virginia.edu/10.1002/jee.20323

Soldatov, A. (2018, March 28). This Is How Easy It Is To Get Hacked. (G. Toboni, Interviewer) Retrieved from https://www.youtube.com/watch?v=G2_5rPbUDNA

Defending and Attributing Cyberattacks
(Technical Report)

The United States' Legal Framework in Cyberspace

(STS Research Paper)

A **Thesis Prospectus Submitted to the**

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Justin Hoon Kim

Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Justin Hoon Kim

Approved _____ Date _____
Advisor Name, Department of Computer Science

Approved _____ Date _____
Sean Ferguson, Department of Engineering and Society

In an age where speed and efficiency have been the primary measures for progress, there has been a mass migration of information and processes to online platforms. As such, there are those who now seek to exploit this shift in medium, attacking cyber structures and frameworks, for their own private gain. With each iteration of vulnerabilities and patches, attacks are only becoming more ingenious and harder to detect. Thus, the ever-growing need for safer cybersecurity measures and a better judiciary procedure is becoming increasingly apparent. (Kosseff, 2018, pp. 987-988).

In 2018 alone, cybercrime generated nearly $1.5 trillion in revenue (HP Bromium, 2018). According to Risk Based Security (2019), 15.1 billion data records were also exposed, a 284% increase from 2018 (p. 4). Furthermore, not only are these attacks very costly, but they are also widespread. A 2019 study performed by Accenture Security determined that nearly 85% of organizations experience some sort of cyberattack, usually in the form of phishing or social engineering, up 16% from the previous year (p. 13). Phishing and social engineering are similar in that they are both means by which confidential information is fraudulently obtained (Accenture, 2019, p. 13). The Federal Bureau of Investigation (FBI) reported they received over 1,200 daily complaints of cyberattacks in 2019 (p. 15). To make matters worse, the ambiguity of the American judicial framework regarding cyberspace makes prosecuting and penalizing cybercrimes unreasonably difficult. According to Kosseff (2018), the US laws surrounding cybersecurity are “an uncoordinated mishmash of requirements that mostly were conceived long before modern cyber-threats” (p. 988). This is largely, in part, due to the “lack of clarity” of the terms “cyber-attack,” “cyber-warfare,” and “cyber-crime” (Hathaway et al., 2011, p. 821). Even in 2018, Kosseff says the meaning of “cybersecurity” has not been properly defined. Thus, most resulting laws are confusing and overbearing (pp. 988-989).

The technical research and tightly coupled STS topic proposed in this paper attempt to provide a better understanding of modern artifacts and frameworks within the cyber realm. On the technical side, I will examine the state-of-the-art cyber capabilities for defending against and attributing cyberattacks. Within the tightly coupled STS topic, I will attempt to unravel the current American legal framework surrounding cyberspace and delineate the contemporary views of how America can improve its cyber legal system. The research will be carried out throughout the spring of 2021.

MODERN CYBERSECURITY

With the guidance of Computer Science professor Aaron Bloomfield, I intend to research state-of-the-art technology within the field of cybersecurity. The term "cybersecurity" is widely understood to mean defending cyberspace from attempted cyberattacks. However, the concept of attributing these attacks to their respective perpetrators is generally lost, even though this step is necessary for punitive measures and, thereby, deterrence (Skopik & Pahi, 2020). Thus, this research paper will outline the most optimal frameworks and artifacts for defending against cyberattacks, and, should they continue to occur, attributing these attacks to apprehend the offenders.

While the US government and its businesses have already begun to invest heavily into the area of cybersecurity, J. Barnes and D. Sanger, two national security correspondents who have written extensively on the subject, conclude that they have not done nearly enough (2020). Cyberoperations "are not yet as central to American national security strategy as nuclear weapons were in the 1950s" (Barnes & Sanger, 2020, p. 3). This growth is essential to win the arms race against "constantly evolving" cyber threats (Cherney, 2020). Otherwise, all online data may as well be considered public information, and individuals, businesses, and governments will

lose vast amounts of money (HP Bromium, 2018). Figure 1 depicts all the costs associated with a successful cyberattack on a system. These costs extend far beyond the mere loss of data but also

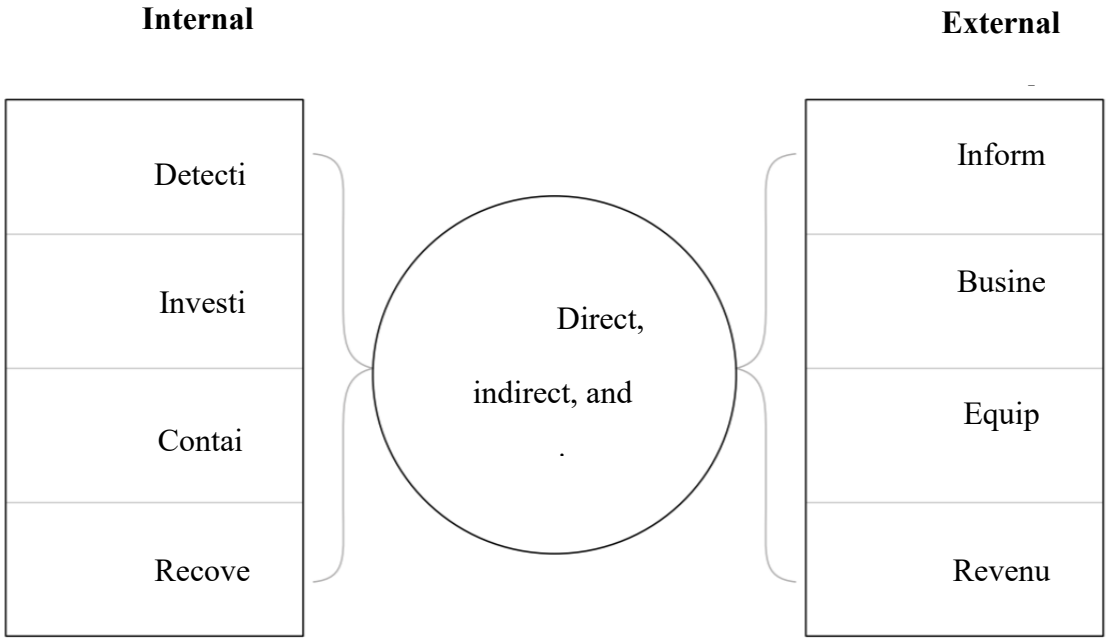


Figure 1: Internal vs. External Costs. The diagram lists the direct, indirect, and opportunity costs of cybercrimes. These costs are divided into internal and external costs depending on whether they are directly related to dealing with cybercrime or the consequences thereof (Accenture, 2019).

include damage control, business disruption, equipment damage, and even revenue loss (Accenture, 2019). Therefore, entities must seriously contemplate the degree to which they ought to invest in cybersecurity.

The general cybersecurity framework, suggested by the National Institute of Standards and Technology (NIST), a non-regulatory federal agency in the United States Department of Commerce, and adopted by many developers, is summarized in five steps. The first is to identify users and individuals who have control over information, creating policies and procedures for security. Then, to protect the system, businesses are recommended to limit access, set up firewalls and filters, patch operating systems, dispose of outdated technologies, and train employees among other suggestions. These suggestions are mainly to eliminate vulnerabilities

and limit risk. The company should also utilize anti-malware and monitor logs in order to detect potential attacks. It is within these last two steps that most cybersecurity artifacts are concerned. Should an attack occur, companies should have a response plan for damage control. Finally, these businesses need to start recovery by taking advantage of back-ups and making any improvements to their technologies (NIST, 2018).

The widespread NIST framework does seemingly neglect the attribution of cyberattacks within its boundaries. This is of no surprise, however, as attribution of crimes is generally within the realm of government and law enforcement. Additionally, according to F. Skopik and T. Pahi, who are affiliated with the Center for Digital Safety and Security at the Austrian Institute of Technology, "cyber attribution is not an easy task" even though it is "a crucial task" (2020, p. 1). The difficulty is only exacerbated by the ease of use of cyber false flag operations. These tactics are applied to "deceive or misguide attribution attempts including the attacker's origin, identity, movement, and exploitation" for the purposes of misattribution (Skopik & Pahi, 2020, p. 1).

In an attempt to resolve the issue of attribution, or the lack thereof, J. Shamsi, S. Zeadally, F. Sheikh, and A. Flowers, who are computer science professors at various colleges and universities, offer the subsequent steps which are also depicted in Figure 2 on the next page: "(1) identification of the cyberweapon used; (2) determination of the origin of the attack; and (3) identification of the actual attacker" (2016, p. 1).

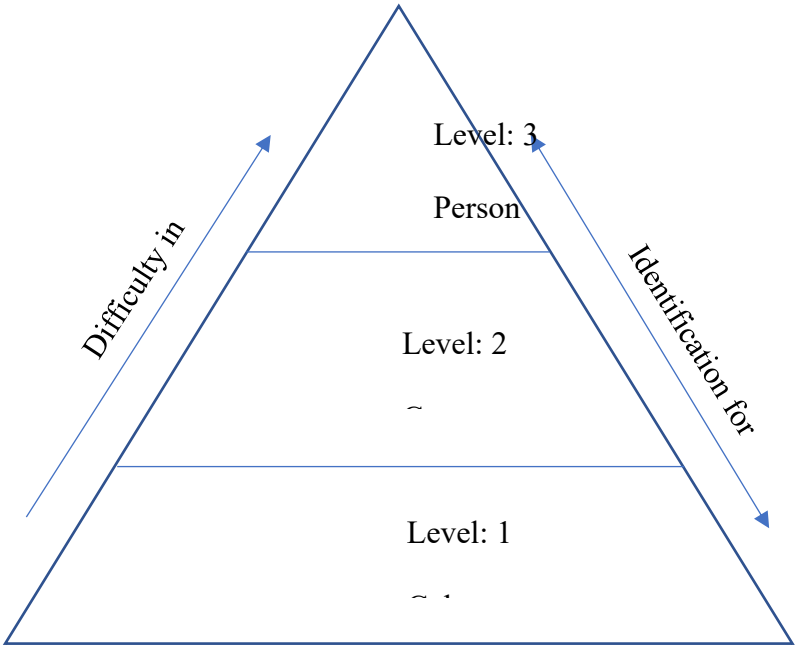


Figure 2: Steps of Cyber Attribution. The figure indicates the progressive difficulty of attributing cyberattacks and all the necessary parts for identifying for attribution (Shamsi & Zeadally & Sheikh & Flowers, 2016).

As can be further be seen from Figure 2, the steps for attribution only get harder as it progresses.

At a very high level, after initial research, the following cybersecurity artifacts are among the most advanced for attribution: tracebacks; honeypots; digital forensics, using static and dynamic data; network forensics; malware-based attribution; indirect attribution, using machine-learning based attribution (Maglaras et al., 2019, p. 6; Shamsi & Zeadally & Sheikh & Flowers, 2016). Many of these artifacts, however, with the exception of indirect attribution, are not very effective against cyber false flags (Shamsi & Zeadally & Sheikh & Flowers, 2016). Thus, to address this inadequacy, F. Skopik and T.Pahi suggest the Cyber Attribution Model (CAM) which "consists of two main parts: cyberattack investigation (part I) and cyber threat actor profiling (part II)" (2020, p. 9). They expound more upon this idea stating:

> Each part consists of technical and socio-political contextual indicators and the components of the CAM approach. The primary aim of the cyberattack investigation is to answer the questions, Who is the victim and Why, as well as What has happened and How. Answering these questions is guided by the components (i) victimology, (ii) infrastructure, (iii) capabilities and (iv) motivation. They help to discover TTPs, the

> modus operandi of a particular cyber attack and required capabilities – and possible false flags (2020, p. 9).

Further, more comprehensive research will be delineated in a technical research paper. The objective of the research work will be to provide a better understanding of state-of-the-art cybersecurity technologies with hopes to increase awareness that will translate into better utilization of these technologies to create more secure and just systems.

COOPERATION OF TECHNOLOGY AND SOCIETY

As long as information is stored online and systems in cyberspace exist, there will forever be cyber threats and attackers. While this is very much a technical issue, there is, without a doubt, a societal and ethical aspect as well. There is the question of how society ought to respond to cyberattacks. What are the ethical boundaries in cyberspace? What actions ought to be taken should the boundaries be violated? And where does the responsibility to protect individuals and society fall?

It is indisputable that there are those in society who are willing to go through immeasurable lengths to violate society's ethical codes for selfish gain. In addition to the previous statistics regarding the revenue of cybercrimes, the Federal Bureau of Investigation (FBI) reports that in 2019, in the US alone, cyberattack victims lost over $3.5 billion (p. 15). This excludes any loss unreported to the FBI. As can be seen from Table 1, not only is there a vast amount of money stolen or lost, but it is generally the weakest and least technologically

Victims		
Age Range	Total Count	Total Loss
Under 20	10,724	$421,169,232
20-29	44,496	$174,673,470
30-39	52,820	$332,208,189
40-49	51,864	$529,231,267
50-59	50,608	$589,624,844
Over 60	68,013	$835,164,766

Table 1: Cyber Victim Losses and Complaints by Age Group. The chart breaks down the total loss and complaints, represented by total count, into their respective age groups. It excludes complaints where age group is not applicable or was not included (FBI, 2019, p. 16).

savvy in society who are the most targeted. The elderly, by far, have issued the most amount of complaints and have suffered the most loss from cyberattacks. Interestingly, the youth, and generally immature, of society, while reporting the least amount of complaints, have lost the most money per complaint. Based on this evidence, the lack of morality of cyber attackers becomes exceedingly apparent, as they target the most vulnerable and susceptible in society. Thus, it becomes apparent that there are technical and societal characteristics within the field of cybersecurity, and it is necessary that these attributes work in unison for the optimal effect.

To demonstrate the necessity, a social construction of technology (SCOT) approach will be taken. This framework emphasizes the relationships between engineers and social groups of certain technologies, stressing that social groups are just as important in the development of technology as engineers (Pinch & Bijker, 1984). As can be seen from Figure 4, the engineer is at the center and has crucial relationships with government, businesses, individuals, attackers, law enforcement and lawyers among others. The centrality is to demonstrate the negotiation that is

facilitated by the engineer between all the stakeholders within the model (Carlson, 2009).

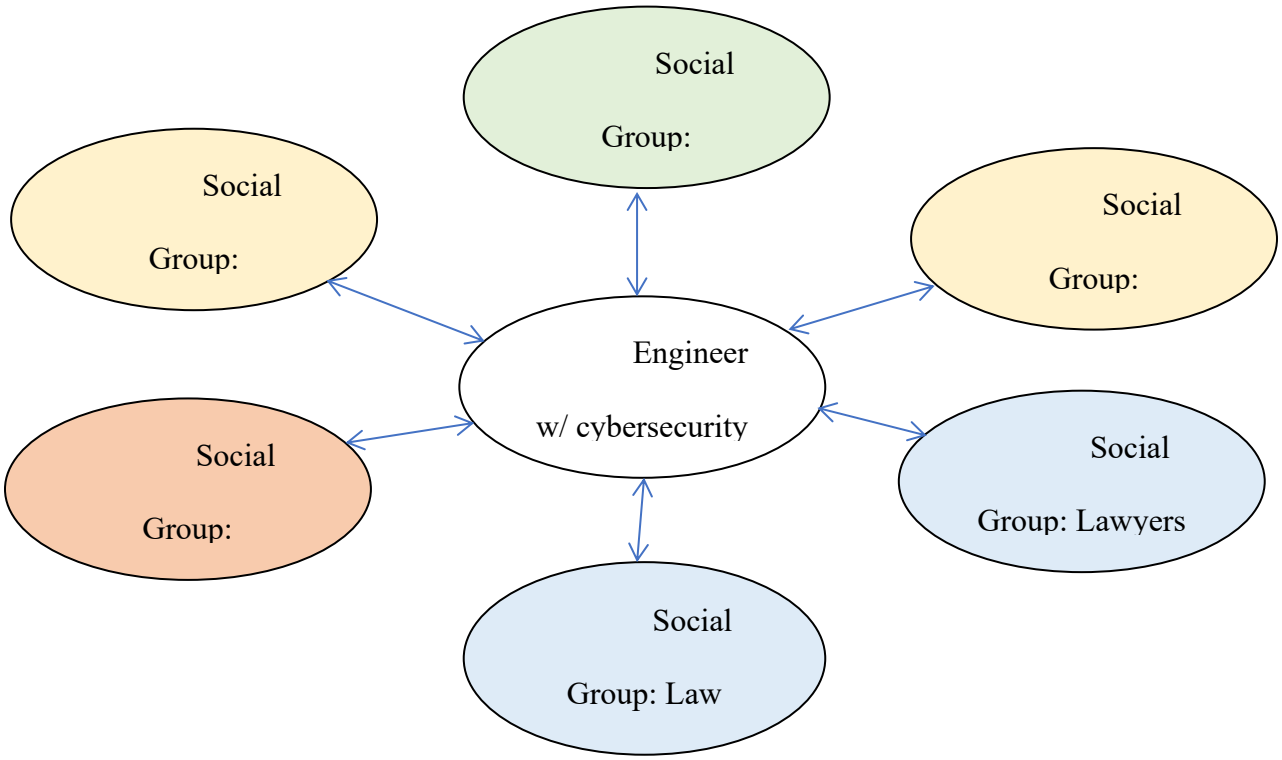


Figure 4: Cybersecurity SCOT model. The engineer is at the center of the social construction. The arrows go both ways to indicate negotiation. The social groups inform the engineer's actions and the engineer provide something to each group (Adapted by Kim, 2020 from Carlson, 2009).

Each of the social groups trusts or, at the very least, expects engineers to perform their responsibilities to provide technical cybersecurity. In the figure, businesses and individuals are yellow to demonstrate they mainly expect secure systems and cyber defense artifacts provided by the engineer. Attackers are red, signifying that they try to exploit and attack the defenses set up by the engineer, creating a need for better cybersecurity. Law enforcement and lawyers are blue to show they mainly rely on artifacts to attribute crimes and provide evidence for prosecution. Finally, government is green to represent that they have an interest in both defenses and attribution (Skopik & Pahi, 2020). These are two-way relationships, however. Thus, the engineer also expects some form of responsibility and communication from the social groups as well. For

instance, the engineer anticipates attackers to create more advanced threats which spurs further innovation. Government, businesses, and individuals are expected to take precautionary and secure measures in the physical world that can work in conjunction with current artifacts (Accenture, 2019; NIST, 2018). Failure of these artifacts should be communicated to the engineer, as well as means by which these technologies should be adapted to fit desired systems. The engineer should also be able to expect cooperation, feedback, and action from law enforcement and lawyers in order to prosecute the cyber criminals (Skopik & Pahi, 2020). The difference in artifacts of security and attribution may create a tradeoff in research, but it is in the power of the social groups to demonstrate necessity and prove a stronger willingness for negotiation.

For the purposes of the tightly coupled STS research, the scholarly article will focus on the negotiation between the government and engineers, specifically examining the cyber legal system within the United States. Unfortunately, "the consensus still is that little can be done to prosecute the perpetrators" even if they are caught (Skopik & Pahi, 2020, p. 1). In other words, there is very little communication between government and engineers, and the United States' government, a major social group in the realm of cybersecurity, is not holding up their end to help shape technology to improve society. As previously mentioned, the United States' legal framework for cybersecurity is inadequate at best. Many laws are unclear, thereby, making it extremely difficult to apprehend, prosecute, and convict cyber criminals. In fact, most laws currently used to prosecute cybercrimes are outdated and were designed for issues unrelated to cyberspace (Kosseff, 2018, p. 988; Office, 2015, p. v, 89-146). These abject legal procedures stemming from undefined terms is unsustainable for the US judicial system (Hathaway et al., 2010, p. 821; Kosseff, 2018, p. 985-989). While the US has taken steps towards defining cyber

terms by passing the Cybersecurity Act of 2015, J. Kosseff, a practicing lawyer and an assistant professor of cybersecurity law at the US Naval Academy's Cyber Science Department, indicates that "the statute fails to provide a concrete definition that sets forth the scope and goals of cybersecurity law" (2018, p. 987). This results in policymakers talking about different concepts when referring to cybersecurity law (Kosseff, 2018, p. 987).

BRIEF PROPOSAL OF DEFINITIONS AND FRAMEWORKS

Therefore, the first step to correcting the US legal system is to properly define the most common words in the context of cyberspace. J. Kosseff begins with the following definition:

> Cybersecurity law promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security (2018, p. 994-1010).

O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, who all have backgrounds in law, define "cyberattack" as an attack that "consists of any action taken to undermine the function of a computer network for a political or national security purpose" (2016, p. 826). Cybercrime is defined to "involve only non-state actors" and must be a "violation of criminal law, committed by means of a computer system" (Hathaway et al., 2016, p. 833). Finally, cyber-warfare "must have a political or national security purpose" and the "effects must be equivalent to an armed attack, or activity must occur in the context of armed conflict" with an objective "to undermine the function of a computer network" (Hathaway et al., 2016, p. 833).

Figure 3 demonstrates the overlap between the definitions of cyberattacks, cybercrimes, and cyberwarfare. Notice that the definition of cybercrime encompasses much more than that of cyberattack and cyberwarfare, and all cyberwarfare is considered to be within the boundaries of cyberattacks.

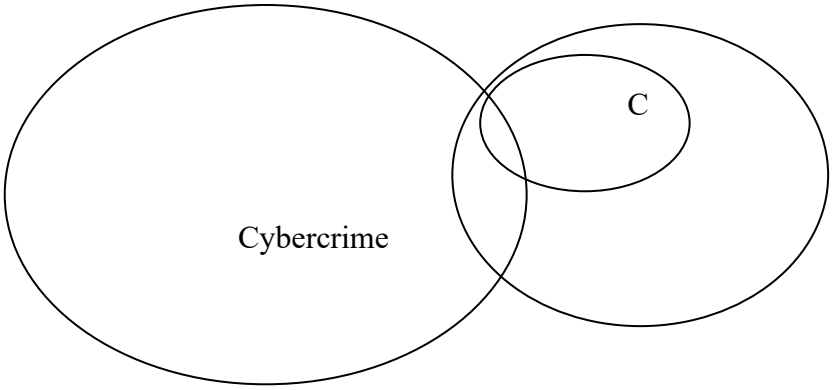


Figure 3: Relationship Between Cyber-Actions. The Venn diagram displays the relationships of the definitions of "cybercrime", "cyberattack", and "cyber-warfare (Hathaway

Working with the aforementioned definitions, J. Kosseff divides the US laws associated with cybersecurity into six categories:

> (1) data security statutes; (2) data breach-notification statutes; (3) data security litigation through common law and statutory claims; (4) computer hacking laws; (5) electronic surveillance laws; and (6) the Cybersecurity Act of 2015 (2018, p. 1011).

Currently, the cybersecurity framework "focuses largely on protecting the confidentiality of information for the purposes of protecting individual privacy" (Kosseff, 2018, p. 1011). However, J. Kosseff argues that this framework should be expanded to include "(1) integrity and availability; (2) protecting systems and networks; and (3) promoting economic and national security interests" (2018, p. 1011). O. Hathaway et al. further "purpose legal reform on both domestic and international levels" to aid with gaps in existing laws (2016, p. 877). Domestically, the US should "add extraterritorial applicability to criminal laws bearing on cyberattacks" and "utilize limited counter-measures to combat cyberattacks" that are not under the category of armed attacks in war (Hathaway et al., 2016, p. 877). On the international stage, the two aims for a cyber treaty include an agreement to limit which cyberattacks can be met with force and

empowerment of “states to cooperate in evidence collection and criminal prosecution of individuals” involved in international cyberattacks (Hathaway et al., 2016, p. 877).

Hence, the cooperation of social groups and engineers is necessary for the success of cybersecurity. With engineers at the center, they must be able to lead the conversation to improve cybersecurity technologies and create a safer cyberworld. The STS research, outlined in a scholarly article, will examine current American legislation surrounding cyberspace and offering appropriate legal definitions and frameworks. The hope is to suggest methods by which the United States can improve its judicial system.

References

Accenture Security. (2019). *The Cost of Cybercrime.* Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Barnes, J. & Sanger, D. (2020, March 11). Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul. *The New York Times.* Retrieved from https://www.nytimes.com/

Carlson, W. (2009). *STS Frameworks*. Retreived from https://collab.its.virginia.edu/access/content/group/8b907a49-dc30-49a0-80f1-12fed136185d/Conceptual%20Frameworks/STS%20Frameworks.pdf

Cherney, M. (2020, October 6). Can Businesses Keep Up with New Cyber Threats? *Wall Street Journal.* Retrieved from https://www.wsj.com/

Federal Bureau of Investigation. (2019). *2019 Internet Crime Report.* Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf

Hathaway, O. & Crootof, R. & Levitz, P. & Nix, H. & Nowlan, A. & Perdue, W. & Spiegel, J. (2011). The Law of Cyber-Attack. *California Law Review, 100*(4), 817-885. Retrieved from http://www.jstor.org/stable/23249823

HP Bromium. (2018, April 20). *Hyper-connected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually* [Press Revenue]. Retrieved from https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/

Kim, J. H. (2020). Figure 4: Cybersecurity SCOT model.

Kosseff, J. (2018). Defining Cybersecurity Law. *Iowa Law Review, 103*(985), 986-1031. Retrieved from https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-3-Kosseff.pdf

Maglaras, L & Ferrag, M. A. & Derhab, A. & Mukherjee M. & Janicke, H. & Rallis, S. (2019, January 12). Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. *EAI Transactions on Security and Safety, 5*(16). doi:10.4108/eai.15-10-2018.155856

National Institute of Standards and Technology. (2018, May 3). *MEP Centers Aid Manufacturers on Cybersecurity.* Retrieved from https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity

Office of Legal Education Executive Office for United States Attorneys. (2015, January). *Prosecuting Computer Crimes*. Retrieved from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Pinch, T., & Bijker, W. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*(3), 399-441.

Risked Based Security. (2020). *2019 Year End Report Data Breach Overview.* Retrieved from https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

Shamsi, J. A. & Zeadally, S. & Sheikh, F. & Flowers, A. (2016, April 26). Attribution in Cyberspace: Techniques and Legal Implications. *Security and Communication Networks, 9*(15), 2886-2900. doi: https://doi.org/10.1002/sec.1485

Skopik, F. & Pahi, T. (2020, March 20). Under False Flag: Using Technical Artifacts for Cyber Attack Attribution. *Cybersecurity, 3*(8). doi:https://doi.org/10.1186/s42400-020-00048-4