Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Melinda Dee Shoemaker

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Raj Singh, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Marcia Kessack, Committee Member,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Attitudes on International Standards for Criminal Hacking in the Public and Private Sector

by

Melinda Dee Shoemaker

MSTS, Eastern Michigan University, 2011

BS, Ferris State University, 2009

Submitted for Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2020

Abstract

There is a current gap in the literature regarding uniform and consistent standards and policies for addressing criminal hacking at the international level. The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for international law defining criminal hacking and the penalties associated with the act. Since the advent of information and communication technologies, there has been a need to address security holistically. The security and sustainability of evolving technologies are examined in light of the threat landscape of criminal hacking, privacy concerns, and policies and laws. Role theory in connection with empathy served as the theoretical base for the research. Data were collected through an anonymous survey of 228 respondents from cybersecurity related organizations from public and private employment sectors. The data analyses resulted in no significance among the groups of employment sectors and the independent and dependent variables, although there were statistically significant results between age groups, gender, infrastructure affiliation, and hacking ability among the questions of the study. Proactively addressing and securing global societies from criminal hacking is paramount in helping to alleviate escalating economic and personal losses among organizations and individuals worldwide. The research insights can be used for positive social change in drafting and implementing cyber policies and laws for criminal hacking among local, state, national, and international bodies.

Attitudes on International Standards for Criminal Hacking in the Public and Private Sector

by

Melinda Dee Shoemaker

MSTS, Eastern Michigan University, 2011

BS, Ferris State University, 2009

Submitted for Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2020

Dedication

I would like to dedicate this research to all the educators throughout my life, including teachers, presenters, and professional colleagues. I would also like to dedicate this research to those who have a desire to grow in knowledge for helping to advance an evolving global society and the good of all humankind for generations to come.

Acknowledgments

A special thank you to those who gave kind words of encouragement throughout the research process and Dr. Raj Singh, my dissertation chair, Dr. Marcia Kessack, my committee member, and Dr. Joshua Ozymy, the university research reviewer for their guidance. I would like to also acknowledge my family for the sacrifices they made during the journey.

Table of Contents

List of Tables

Chapter 1: Introduction to the Study

Today's virtual landscape has consistently evolved with the advent of newer and emerging technologies. There is a need for legislative bodies, law enforcement agencies, and public and private sector organizations to make significant strides in collaboratively addressing security issues that have escalated from the exponential technological growth over the past several decades. Ghernaouti (2013) illustrated the vastness of information and communication technologies (ICT) and the power they enable. This power is achieved on both sides of the legal spectrum, while the ultimate power can be described as the ability to harness the digital technological infrastructure realm for responding to various machinations (Ghernaouti, 2013). Dixon (2007) showed there is more to addressing security issues in the information technology realm, which surpassed the use of technologies to secure the environment and encompassing a comprehensive approach to education and policy.

The cyber world has no boundaries and the interconnectivity of technologies has posed many threats. Multinational efforts, including the United Nations, the Group of Eight, International Telecommunications Union, and the Organisation for Economic Co-operation and Development, have addressed cybersecurity and critical infrastructure protection toward a global standard approach, which will take time (Segura Serrano, 2015). More specifically, there is a need for consistent multinational collaboration in the policy realm for clearly defining criminal hacking and the punishments for committing these crimes.

Oh and Lee (2014) explained the need for specificity in the realm of criminal law for penalizing acts of criminal hacking. Oh and Lee (2014) found that the degree to which hacking crimes are penalized should be closely evaluated, due to the variations of the crime and the damages caused, to help in determining appropriate punishments. In their study, Oh and Lee (2014) evaluated the attitudes of respondents in the public and private sectors through anonymous individual surveys, focusing on the development of a consistent international standard that would serve as the rule for global societies in defining and prosecuting acts of criminal hacking to glean insight or new knowledge that could be used for future studies.

The world has changed and evolved in the way global societies function on a daily basis, including the usage of many technological devices that create vulnerabilities and risks for the user. Buchanan (2016) showed how the "cybersecurity dilemma," which encompassed defensive and offensive intrusions among nations and the sometimes-unintended consequences that resulted in these acts. This illustrated only a piece of the holistic picture that represented technological intrusions and potential ramifications involved in the virtual realm.

All users of virtual technologies need to be aware of the vulnerabilities of the technologies and how risks, involving the security of individuals, properties, organizations, and nations come into play. Cavelty, Mauer, and Krishna-Hensel (2007) explored documentation from the World Summit on the Information Society from December 12, 2003, which stated the action plan of coordinative efforts among the public and private sectors to address cybercrime issues and legislative implementation, while

promoting initiatives for educating the population toward being aware of the threat landscape and building a security culture. This chapter provides a synopsis of the background of the connecting elements of the study, which included the threat landscape of criminal hacking, security issues involving virtually connected devices, privacy issues in relation to criminal hacking, and the challenges of global coordinative legislative efforts for creating and implementing legislation for the punishment of criminal hacking. Additional sections for the chapter provide a comprehensive foundation for the study.

In the realm of cybersecurity and policy, there is a need to explore individual public and private sector attitudes toward having an international law that defines criminal hacking and the penalties associated with the crime, so legislative efforts can better address the problem of criminal hacking in the cyber realm. McDonald (2002) explained how risks and uncertainty have substantially increased on the global scene due to all processes involved in globalization. Although many insights have been studied, McDonald (2002) concluded that a successful policy approach toward a democratic governance response will entail considerations that include proactively engaging interactions among the public administrators, while understanding our fallibilities. This study provides a framework that connects the threat landscape of criminal hacking with the security of global networks and connected technologies, and the security and privacy of all who rely on connected technologies in the modern-day era to help promote uniform policy solutions for the punishments of criminal hacking.

The theoretical foundation for the study is role theory, in tandem with an illustration of critical policy issues, which was used to examine the urgency and

obligations of future generations and the well-being of global society. The research questions in this study were used to examine attitudes toward the need for establishing an international law for a global definition of criminal hacking, attitudes in establishing an international law for regulating punishments for criminal hacking activities, and attitudes toward the extent criminal hacking should be penalized. Definitions for the study, assumptions, scope and delimitations, limitations, and the significance of the study can be seen from the brief synopsis provided on the criminal hacking threat landscape. A holistic overview of the connecting entities that comprise interdisciplinary and multidisciplinary domains was used to address the problem of the study in Chapter 1, which provides a foundation for a detailed examination of the connected pieces in Chapter 2.

Background

The background briefly summarized literature in relation to the study of criminal hacking and policy efforts toward creating and implementing legislation and for the crime, the threat landscape of cybercriminal hacking activities in relation to privacy and security, and why there is a need to study multinational standards for the punishments of criminal hacking. The scope of the study fell under the umbrella of cybercrime, which embodies many categories and methodologies. The study specifically addressed the crimes of hacking and the penalties associated with the crime, while the attitudes implementing effective policies and laws on an international level were examined.

When developing policies and laws, there is a need to holistically understand the elements intertwined within the problems being addressed. To better understand the

evolution of hacking, the following is an introduction to what has become a multibillion-dollar criminal activity worldwide (Internet Security Threat Report, 2017). A glimpse of the speed at which the technological landscape has matured and morphed is illustrated, and vital elements lay a critical foundation for the study.

Examples of cybercrime can be seen as far back as 100 years ago, described Hill and Marion (2016), with a cyber-hacking incident involving Morse code. Nevil Maskelyne, an inventor and magician, born over 150 years ago, hacked a demonstration of the emerging technology of Morse code at London's Royal Institution Theater in 1903 without the knowledge of the demonstrators, John Ambrose Fleming and his friend Guglielmo Marconi (Hill & Marion, 2016). Maskelyne intercepted the Morse code message and changed it to display something other than that intended, which showed the audience the technology was vulnerable to security issues, including privacy (Hill & Marion, 2016). The Morse code example shows how humans can figure out inventions and manipulate them for various reasons and motivations.

The Internet of today is young in comparison with technological advancements over the past century (Hill & Marion, 2016). Hill and Marion (2016) elaborated on the evolution of the Internet, being initiated over 50 years ago, with the use of technologies developed for the military and research purposes during the Cold War to prevent the Soviet Union from continuing their technological lead after being the first to launch a satellite into space. The Advanced Research Projects Agency (ARPA) and the information processing techniques office had the ability to share information through computer interconnectivity, which did not become fully used until the Advance Research

Projects Agency Network (ARPANet) was created (Hill & Marion, 2016). These technological advancements enabled the creation of the Internet in 1990 and created new avenues for the criminal world to thrive (Hill & Marion, 2016).

Although computer crimes were minimal throughout the 1960s through the 1970s, due to computer usage being primarily restricted to researchers and the military, hacking activities took place, mainly by curious students who wanted to better understand the technological environment showcasing their skills to be able to break into something designed to be secure (Hill & Marion, 2016). Hacking offenders oftentimes would sign virus intrusions with their names, due to their confidence and the lack of laws for the criminalization of these types of activities (Hill & Marion, 2016).

Hacking activities and the criminalization of hacking has evolved since the 1960s and 1970s due to the escalation of computer crimes and the implementation of policies and laws in the cyber realm. Hill and Marion (2016) showed how during the 1970s the motivations of hackers began changing from an inquisitive nature to more malicious and damaging. Hill and Marion (2016) identified a computer crime in the 1970s, including the manipulation of computer data at the Union Dime Savings Bank in 1973 for embezzlement.

The 1970s gave rise to a hacking technique called *phreaking*, which involved the technological skills of hackers to break into phone systems, using tones and the codes from the system to gain access to free long-distance phone calls (Hill & Marion, 2016). At the Flagler Dog Track in Florida, tickets were altered to produce winning numbers, which led the Florida computer Crimes Act of 1978 to define accessing a computer

without authorization as a crime (Hill & Marion, 2016). The Federal Computer Fraud and Abuse Act was passed in October 1986. More details on this legislative act and how criminal hacking has progressed over the last several decades will be in Chapter 2.

Criminal hacking has greatly contributed to data breaches and cybercrime, in general, over the last couple of decades and continues to escalate. Hampson (2012) provided information on how billions of dollars are lost each year due to criminal hacking. The Internet Security Threat Report detailed how cybercrime is growing exponentially every year and the loss from data breaches in 2017 consisted of more than one billion personal records being compromised, and this is only what has been reported, as companies often choose not to report the entirety of their breach (Symantec, 2018). Symantec's (2017) study also indicated that approximately seven billion identities have been stolen over the past 8 years, approximately the number of the global population today.

Nash and Thomas (2006) explained that approximately three fourths of the experts in the security realm of IT believe that cyber criminals are prevailing due to a lack of international laws, law enforcement resources, and lack of overall global participation and cooperation in addressing the importance of hacking crime. Pollaro (2010) provided information on how the Federal Computer Fraud and Abuse Act has been revised to broaden its scope as a statute from the U.S. Federal Computer Fraud and Abuse Act, that once primarily addressed hacking of government computers but now addresses hacking of any computer connected to the Internet. Kain (2013) argued that the Federal Computer Fraud and Abuse Act has resulted in a patchwork system that is not

uniform. Concerted efforts among international stakeholders are needed to help address inconsistencies surrounding criminal hacking policies and deterrence.

Goodman (2015) explained how societies depend on the technological interconnectivities that enhance quality of life, whether through convenience or efficiency, but with these continuously advancing technologies comes many vulnerabilities. The growth of technologies coincides with Moore's law and the effects that come with the use (Goodman, 2015). Moore's law will be examined in Chapter 2. There is a dark world of hidden criminal activities within the universe of borderless virtual boundaries and all the intricacies involved (Goodman, 2015). Holistically understanding what is happening in the virtual world, through the help of international technical experts, could help in determining what the best course of action would be for future policies addressing cyber-criminal activity.

The Global Forum on Cyber Expertise (2017) interviewed Lynn St. Amour, chair of the Internet Governance Forum, which advises the secretary general on the Internet Governance Forum meetings. The Internet Governance Forum, founded in 2005, now has approximately 55 interdisciplinary worldwide organization members, including public and private sectors, academia, technical organizations, and civic society, who collectively deal with Internet governance issues on the global scene. St. Amour responded to a question about what the future holds for the Internet over the next decade by explaining how the growing *Internet of Things* (IoT) and technologies using blockchain will have an even greater impact on society than the present focus of the financial markets. St. Amour expounded on how 50% of the world that is not connected

to the Internet now will increase, moving toward a technologically mobile device concentration that is multifaceted, making up the future of the Internet (Global Forum on Cyber Expertise, 2017). This growth will add to the complexities involving technological security and the policies crafted in addressing the acts of criminal hacking.

Burkart and McCourt (2017) identified the security and privacy concerns with packaged software being developed and distributed in markets that have minimal regulation in the technological realm for the purposes of online surveillance. The European Union addressed, through policy, the protection of personally identifiable information in the form of a framework, which regulates marketing of personally identifiable information (PII; Burkart & McCourt, 2017). This type of framework has not been implemented in the United States, although these issues may be addressed through self-regulation in industry, which could help in the implementation of international treaties addressing trade in these markets for curtailing various security and privacy concerns, stated Burkart and McCourt (2017).

Roberts (2013) argued that leaders will need to recruit and teach strategic cyber thinkers, so there can be proactive efforts in gathering international support to catch and prosecute criminal hacking activities. Theohary and Rollins (2009) illustrated how many issues have challenged the United States, including not knowing for sure where the perpetrators committing various cyber-attacks are located. A lack of federal-private sector coordinative efforts in determining potential risks and new increasing threats at the international level poses the continued possibilities of national critical infrastructure

disruptions, which suggests the need for enhanced strategies and updated policies (Theohary & Rollins, 2009).

Brown and Poellet (2012) showed how customary international law vastly differs from the case law system, making proposals for universal legislation extremely challenging. Trivun, Mahmutćehajić, and Silajdžić (2012) warned that the only way the Internet architecture can be properly maintained and secured in this global environment is total collective participant in regulation development and implementation. The results of this study can help in coordinating efforts toward the creation and implementation of effective policies for criminal hacking, while providing relevant research of the current threat landscape of criminal hacking.

Problem Statement

The overall receptiveness and acceptance of technological advances over the past several decades, from the Internet to the numerous applications used to make everyday lives easier, have created a global dilemma. By readily accepting, and in many cases, embracing, these technologies without fully understanding the security risks and implications involved, a global threat landscape has developed in the virtual realm, which lacks consistent regulations and controls. The lack of consistent regulations and controls throughout various global jurisdictions has contributed to the difficulties in finding the true origins of computer intrusions and bringing to justice those responsible under a criminal justice system that deals with the problem consistently at all levels of government.

The global community is arguably past due in having consistent established policies and legislation that specifically address the penalties and punishments of hacking activities in the information technology realm. Greengard (2012) suggested that nation states more lenient in their legislative practices toward the criminal behaviors of hacking may be opening up, if not already providing, a haven for hackers. Nash and Thomas (2006) explained that the growing problem of hacking continues to be detrimental to societies worldwide, and legislative actions among various nation states have not been able to fully address the problem. Hampson (2012) showed that various acts of hacking are responsible for crippling world economies, with losses of billions of dollars every year.

There is a current gap in the literature regarding uniform and consistent standards and policies for addressing criminal hacking at the international level. No clear definition for criminal hacking or agreement on punishment for the crime pose a number of challenges, negatively affecting the sustainability of evolving technologies. In this quantitative study, I explored individual public and private sector attitudes toward the need for one international law for defining criminal hacking and the penalties associated with the act and the extent to which the crime should be penalized.

Purpose of the Study

Criminal hacking has been taking place for decades. Billions of dollars have been lost due to criminal hacking and the costs continue to escalate. Security breaches are only one aspect of the problem. The Symantec 2016 Internet Security Threat Report stated there were 1,209 breaches in 2016, up approximately 25% since 2013 (Symantec,

2017). The report also stated an average of 927,000 identities were exposed per breach. A security breach involves many elements that harm individuals, businesses, and the global economy. There are multifaceted criminal uses for the information obtained through these breaches. The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for one international law for defining criminal hacking and the penalties associated with the act.

The criminal world has created an opportunity of cyberspace to accomplish exponential gains. Mitchell (2016) stated that hacking attempts worldwide surpassed one billion in 2012 according to a study by the British security firm NCC Group. The complexity of curtailing crimes taking place in a virtual environment without an established system for controlling those criminal activities continues to grow.

Effectively securing networks and technological devices is essential. Buchanan (2016) delineated how the international arena is comprised of computer hacking for intelligence gathering through the intrusion of various networks in the public and private sectors. These intrusions can be avenues for attacks capable of manipulating and destroying data (Buchanan, 2016). Buchanan further stated that, through digital forensic reporting, it is evident there are intrusions being employed on the national scene for more than defensive and training purposes, although not all nation states have the capabilities for this. The sense of urgency among international communities has not been compelling enough to reach international solutions to curtail criminal activities in cyberspace (Fidler, 2016).

Through scholarly research, an examination of the threat landscape, privacy and security, and multinational policies and laws provided a foundation for the focus of this study. The relationship among public and private sector individuals and their attitudes toward one international law for defining criminal hacking and subsequent punishments were explored, which provided insights that could help propel global policy awareness toward addressing the virtual threat landscape of criminal hacking. Additionally, the insights gained determined the need for an enhanced approach to address policy and law for criminal hacking through increased coordinated efforts with multinational and international laws regulating the criminal hacking realm. In this quantitative study, I used an anonymous survey to examine attitudes among public and private sector individuals on the need for one international law for defining criminal hacking and the degree of penalties for committing the crime. Statistical tests of the data revealed a correlation among some of the variables of the study, which provided some statistical significance among the attitudes of the respondents.

Research Questions and Hypotheses

The research questions for this quantitative dissertation were designed to gain some insight from public and private sector individuals on their attitudes toward the need for an international law defining criminal hacking, the penalties associated with the act, and the extent to which it should be punished. The independent variables of the study included age group, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education, which related to the hypotheses by providing, through correlation, what the relationship was among the groups of public and private sector entities for the

variables of the study. The central research question is: Is there a need for the definition of criminal hacking and the penalties associated with the act to be addressed under one international law?

RQ1: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector entities?

$H_0$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector individuals?

$H_1$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector individuals?

RQ2: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_0$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_1$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

RQ3: Is there a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_0$3: There is no difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_1$3: There is a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

Theoretical Foundation

The threat landscape of criminal hacking played a significant role in the security of networks and technologically connected devices and the security of individuals and their privacy. The threat landscape, in relation to the holistic security of individuals and

all connected technologies, provided a foundation for the need to develop and implement universal standards for the punishments of criminal hacking using the frameworks of role theory and empathy in political theory.

Trivun et al. (2012) pointed out that regulation encompassing the architecture of the Internet cannot be determined by individual entities, but rather it must involve authorities at all levels, relying on economic and political entities at the local, national, and international level. Trivun et al. (2012) showed how the Internet acts as an international framework that could unite various regions of the world to work together in harmony, while addressing various security issues present. This framework, according to Trivum et al. (2012), is comprised of entities at the lowest levels in government and those at the highest levels and cannot be separated from traditional laws and theories of law that have governed communities before the advent of the Internet.

Menon and Siew (2012) showed how a unified multilateral effort is needed to address cybersecurity issues, which play a significant role in the future and security of the global economy. Newman and Thakur (2006) illustrated how global societies are vulnerable to many of the same problems that each entity faces separately in relation to a number of global issues. There is more efficiency in multiple coordinative efforts for the common good of the world rather than unilateral or stand-alone efforts, even with the limitations that come with the holistic approach (Newman & Thakur, 2006). A closer look at these efforts offers insight into where policy initiatives are underway in addressing criminal hacking. Furthermore, foreign policy in the context of international

relations provides an aggregate illustration in relation to these different political cultures in Chapter 2.

Role theory, as demonstrated by Thies (2009), served as an umbrella theoretical framework for this study in the context of international governing entities. Given that the nation-state system is understood through the lens of international relations, role theory helped contextualize how hacking has been approached at the international level. This theory, projected through an exploratory lens, helped explain the role of foreign policy and its connections to public administrators (Below, 2014). The use of role theory in this study provided a model for positive social change toward international coordination efforts in addressing policy issues surrounding criminal hacking for clearly defining the act of criminal hacking and the punishment standards for the act.

An examination of empathy in political theory, as posited by Edge (2016), showed how empathy is a key component missing in the political landscape today, and it may offer some hope in addressing future international initiatives. The phenomena that provided a foundation for the study encompassed pieces of a conceptual puzzle, which included the security of everything technologically connected and the privacy and security of everybody in the virtual realm and policies and laws in relation to the cybercriminal threat landscape of criminal hacking. From these concepts, relative proposition statements showed how the puzzle pieces, figuratively speaking, are connected and related through the theoretical veins of role theory and empathy in political theory. These theories, as separately illustrated in the literature, are examined in Chapter 2.

In this study, I explored criminal hacking through a framework that used the current threat landscape in the virtual realm as a magnifier for determining if there is a need for an international law defining criminal hacking and the penalties associated with the act. Logical connections for this study have been illustrated through the threat landscape of criminal hacking, which includes categories and methodologies. Security and privacy issues have been connected in relation to criminal hacking, furnishing evidence that addresses the deficiencies of multinational policies and laws for the punishments of criminal hacking. This framework provided significance to the problem at hand while offering key concepts that work in conjunction with the theories used, which supply insight for the questions of the study. The connections are analyzed and covered in Chapter 2.

Nature of the Study

A quantitative approach was used for the study. Qualitative studies can be more complex in the interpretive arena and rely on statistical analysis and testing methods. In this research, I took a pragmatic approach, using breadth to add to the validity and strength of the study. The scope of the study incorporated quantitative methods for empirically focusing on descriptive statistics to evaluate audience segmentation and opinions for the hypotheses tested in attempts to garner information universally. The study combined empirical and theoretical aspects, which provided a comprehensive picture of the phenomena, while the questions of the study established predictions and material for future studies that choose to use quantitative and qualitative methods.

It is important to understand basic meanings of the foundational verbiage used throughout this dissertation. A few explanations involving the threat landscape, criminal hacking, and personally identifiable information are given to clarify these concepts and phrases, for the purpose of this study. The following provides definitions for these key terms.

Definitions

Threat landscape: For the purpose of this study, the concept of the threat landscape refers to the acts of criminal hacking and the methodologies used.

Criminal hacking: Unlawful hacking, according to the laws put in place in any particular jurisdiction.

Personally identifiable information (PII): Any type of information that identifies or can help to identify an individual. The U.S. Department of Homeland Security Privacy Office (2002) distinguishes between *PII* and *sensitive PII*. The European Union differentiates PII data as being personal data or sensitive data (General Data Protection Regulation, Art. 4).

Assumptions

The quantitative paradigm assumptions include questions that should be answered ontologically, epistemologically, axiologically, rhetorically, and methodologically (Creswell, 1994). The ontological assumption addresses the question of reality, which is objectively examined. The epistemological assumption provides a distinction that a researcher will be independent from the research. The axiological, or role, assumption shows that the research is unbiased and free of values. The language of the research, or

the rhetorical assumption, shows a formal and quantitatively impersonal stance. The methodological assumption includes the research encompassed a deductive process through generalizations, validity, and reliability.

The following assumptions are noted for the study: First, most technologies are vulnerable to criminal hacking. Second, a security awareness culture will help alleviate some of the vulnerabilities encountered from criminal hacking activities through the implementation of best practice standard protocols in securing technologies. These assumptions were necessary and provided the reader with general assumptions recognized by many cybersecurity professionals and interdisciplinary and multidisciplinary practitioners.

Scope and Delimitations

The scope of the study is limited to the defined acts of criminal hacking and the laws for the penalties associated with the crime. *Cybercrime* encompasses a vast array of elements that would fall outside of the realm of criminal hacking, including cyber bullying, child solicitation, identity theft, and cyberstalking; elements of criminal hacking do come into play with all these crimes. Wilsem (2013) illustrated, how crimes that are computer-focused, "…such as virus, malware or botnet infection, and hacking (as cited from Furnell, 2002, p. 22)," solely depend on the technological realm, whereas computer-assisted crimes consist of crimes that took place before the inception of the Internet but use technologies to commit crimes today. In this research study, I focused on the acts of criminal hacking, the methodologies used, targets of the crime, and legislative efforts and implementations for the punishments of criminal hacking.

The populations for the study included interdisciplinary and multidisciplinary individuals involved with the technological arena of cybersecurity in the public or private sectors, cyber legislation realm, law enforcement, or academia. This study excluded the general population due to scope and limitations; future studies could gain a broader insight by conducting a study of the general population from a multinational population. I chose this focus because societies are past due in clearly defining and addressing the penalties for the criminal acts of hacking in the virtual realm. Insights gained from this study may help propel future studies in the policy realm by generating additional knowledge to better understand attitudes among the public and private sector on the need for international laws for criminal hacking.

In regard to generalizability, Barnes et al. (2012) showed how predictions for the findings of a quantitative study cannot serve as being precise due to the sample size, the interpretations of the sample in relation to the understanding of the questions being asked of the population, and the baseline of the predictability and assumptions to similar or past occurrences in the field of study. Barnes et al. (2012) explained how researchers should consider using a precise external measurement process that consists of three categories of generalizability, which include treatment measurement and subjects to add to the reliability of the study; however, doing so does not guarantee similar results will be obtained if applied outside the study. Scope and variance are examined in a quantitative study.

Limitations

The motivations of all criminal hacking incidents cannot be clearly defined, which makes it challenging to address the penalties needed for various acts of criminal hacking. According to the definition of the laws in place in different areas of the world, it remains unclear if all criminal hackers possess a mindset for committing a criminal activity. It is also unknown what part culture plays in various areas of the world toward the mindset of committing criminal hacking. This study is based on information available to the public, which alleviates classified information in the global arena. Policy information is also limited to nation states that are open with their policies. Criminal hacking activities and those that have been compromised are limited to what has been reported.

Available scholarly research has been examined to help provide a model in delineating some of the motivations behind criminal hacking to contribute to the elements needed for formulating a consistent standard policy for the punishments of criminal hacking globally. Global policy initiatives may benefit from research that expounds on the consistencies and inconsistencies in punishments of criminal hacking on a multinational level, offering some insight into issues surrounding the challenges and intricacies of developing standard policies in the virtual realm. Some implications of the study offered the opportunity for positive social change in the realm of policy and legislation, which can be drawn from the possibility of future studies in building on and adding to this study in the realm of conviction rates for criminal hacking and the recidivism rates of criminal hacking.

Significance of the Study

Global societies have been working on how to deal with the creation and implementation of effective policies in relation to cybercriminal activities that have been escalating for decades. By peering through the lens of the threat landscape of criminal hacking, security, privacy, policies, and laws, the connected concepts have been examined to provide an epistemological overview of the ontology of criminal hacking. These taxonomies have shown how each provides connecting threads toward building effective solutions for mitigating the problems associated with criminal hacking.

There is a critical need to address the issues of criminal hacking at all governmental levels and at the international level, so that no individuals or groups have immunity from prosecution and conviction for criminal hacking activities (Greengard, 2012). This study contributes to the body of knowledge needed to address the problem through an examination on the attitudes of public and private sector individuals toward the need for clearly defining criminal hacking and the extent punishments should be associated with the acts.

Hacking activities have accelerated with the use of hardware and software technologies and the intricacies of the Internet and its connected networks, and the global costs escalate. Hathaway (2014) evaluated the implications for regulating various aspects of the Internet, and many existing policy challenges are deep-rooted within the foreign policy realm. This study's positive social change implications include the identification of optimal legislative strategies and best-case practices in enforcement that bring the world closer to uniform policies for various kinds of criminal hacking. Consequently, the

study serves as a guide to parallel legislation at the level of the nation state and may eventually support international treaties that establish uniform standards and a global regime to combat criminal hacking.

Implications for Positive Social Change

There is hope this study will motivate researchers to continue with similar studies in addressing the issues surrounding the new era of technological growth and the implications it has on global societies in efforts to help promote potential solutions in combating criminal acts in the ICT realm. By understanding the threat landscape in the virtual realm and the negative consequences of various hacking crimes, coordinative efforts among public and private sector entities have provided additional insights for legislative bodies worldwide to band together and move forward in clearly defining and regulating the criminal acts of hacking.

Summary

In this study, I looked at how role theory plays an integral part in addressing the fundamental problems of technological compromise, while providing a foundation for analyzing the current threat landscape of criminal hacking, and determining if there is a need for an international law for defining criminal hacking and the penalties associated with the crime. The quantitative empirical study approach consisted of descriptive and inferential statistical research, offering elements of audience segmentation and the ability to quantify the perceptions, attitudes, and opinions of the sampling units, while generalizing the relationships between the independent and dependent variables of the study, which were used to gain insight and propose questions for future studies in the

political legislative realm. The security of global societies depends on swiftly addressing the problems that encompass our technological realm. In Chapter 2, the connecting elements of the criminal hacking threat landscape, the security of networks and connected devices, privacy internationally, and the multinational efforts in creating and implementing legislation for the punishments of criminal hacking are examined.

Chapter 2: Literature Review

Introduction

Modern societies are experiencing exponential technological growth and with that comes uncertainty for the threat landscape of vulnerabilities and privacy and security concerns. The purpose of this study was to provide insight on attitudes toward a holistic approach in addressing the threat landscape of criminal hacking through international laws clearly defining criminal hacking, policies associated with criminal hacking, and penalties for the crime. Given the virtual landscape has no given boundaries, various international entities have come together to propose solutions for addressing the problem, but no general consensus has been reached on how to proceed forward in defining and addressing acts of criminal hacking and determining whether a need exists for a global standard for policies and penalties associated with the crimes.

In Chapter 2, the following topics are discussed: a literature search strategy, a theoretical foundation for the study, a literature review tying in key variables and elements of the study, and a concluding summary of the fundamental paradigm of the policy dilemma. A strategic approach was taken to exhaustively search the literature to gain a holistic international insight to address the questions of the study, and the gap in the literature was examined for the problem of the study.

Literature Search Strategy

The Walden University databases were accessed using various search engines in relation to the study, including Political Science Complete, Criminal Justice Database, SAGE Journals (formerly SAGE Premier), LegalTrac, LexisNexis Academic, Military

and Government Collection, Homeland Security Digital Library, Science Direct, and Thoreau Multiple Database Search. Key search terms, with the utilization of various search combinations, were *regulation, law, policy, legislation, universal legislation, hacking, computer intrusion, ethical hacking, computer crime, cybercrime, cyber security and cybersecurity, role theory, deterrence theory, punishment, public policy, international legislation, foreign policy, international relations* and *cybersecurity law*.

I performed an initial search of the connecting elements of the study to ensure foundational works within the scope of the study were available. Most of the research for this study consisted of peer-reviewed journal articles, books, and conference proceedings covering the last 5 years; some research is provided from earlier writings of subject matter experts. The Institute of Electrical and Electronics Engineers (IEEE) is known for setting standards in the electronics and computer industries. IEEE provided documents on conference proceedings in relation to the study.

Theoretical Foundation

With a global environment that is virtually connected, addressing policy solutions in the virtual realm will need the perspectives from multiple stakeholders. Trivun et al. (2012) pointed out that regulation in relation to the Internet and modern-day technologies should be approached from a holistic stance, including all political entities from local, national, and international levels, to be able to fully address the intricacies involved. This multinational, multidisciplinary approach could unite various regions of the world to work together while addressing the threat landscape of the virtual realm. A body of international leaders and experts should establish a policy framework to see the benefits

of addressing role theory in connection with the roles played in leadership. These leaders should enact those roles with expedient action and empathy, serving as an influencing stimulus for all entities to model in the virtual realm.

Role Theory and Empathy

Role theory provided a theoretical foundation for this study with the consideration of empathy. Thies (2009) showed the need for international communities to take the role of working together to address policies through international relations, while Edge (2016) showed how empathy is missing in the political environment of policy development. Within the role theory construct is an illustration of applying an empathetic model approach for addressing policy standards for the international community in the realm of criminal hacking (Edge, 2016). Empathy can furnish a missing piece in international policy strategies by embracing a genuine concern for the welfare of all entities involved in the policy development process.

Looking through the lens of empathy while fulfilling a political obligation to work in concert with international bodies may propel a holistic consideration for examining the reasons and motivations of criminal hacking and potential solutions for addressing the problem other than potential incarceration as a deterrence method. A multidisciplinary approach, including the involvement of subject matter experts in relation to the many elements involved, for considering a holistic international framework that provides consistency and resiliency as the standard for all environments encompassing the virtual realm (Trivum et al., 2012). Efforts should include a holistic approach of addressing the elements of the virtual threat landscape of criminal hacking, the security of

technologically connected devices, global awareness strategies for further addressing the privacy and security of our global citizens (Menon and Siew, 2012).

Bonner (2016) illustrated how the role of actions in role theory depends on the actor, with expectations coming into play as to what actions should be taken. Controversial outlooks of the past, according to Arendt's evaluation of what the action role has in role theory, showed how role theorists looked objectively, rather than taking an ethical approach, to political circumstances of action, which can be seen from the atrocious acts committed throughout the centuries by those with political power playing no empathetic role to achieve their agenda (Bonner, 2016). Today role theory can be seen as a theoretical approach to applying expected actions to the roles given in leadership, where it is expected that those with decision-making powers will fulfill their roles in efforts to protect the population (Wehner & Thies, 2014). In this study, role theory will provide a model for positive social change toward international efforts in addressing policy standards and laws for criminal hacking.

The link to empathy in role theory provided an approach for examining future international policy and law development through multinational coordinative efforts in relation to the attitudes of multidisciplinary entities. This study consisted of a holistic approach in tying the pieces of the current threat landscape of criminal hacking with the elements of privacy and security and the attitudes toward an international approach in establishing international laws for clearly defining criminal hacking and the policies and penalties associated with the crime. The holistic framework provided significance for addressing the problem of inconsistent policies for criminal hacking, while the theoretical

foundations of role theory and empathy serve as a foundation for the questions of the study on whether a need exists for one international law defining criminal hacking and the punishments associated with the act.

Moore's Law

Moore's law provides implications and relevance to the problem of this study by addressing the speed at which technologies evolve. Goodman (2015) showed how Moore's law, which shows technological growth doubling every 2 years in relation to computer processing chip components, has continued the predicted path over the years, although DeBenedictis (2017) delineated, citing Moore (1965), how Moore's original 1965 article is broad in scope and there are modern-day inconsistencies. Nonetheless, Moore's law should continue to be recognized as a positive factor for the computational growth in the technological realm moving forward.

Over the past 50 years there has been an evolution, in relation to the technological growth of semiconductors and computers, described DeBenedictis (2017), enabling for our technologies to surpass the original concept of Moore's law, to include newer technological developments that fall outside of the original scope of Moore's law, such as with 3-D manufacturing and neuromorphic circuits, quantum qubits, and newer computing memory techniques. Denning and Lewis (2017) stated how technology in relation to components, speed, and technological modernizations are normally applied to Moore's law, although the only one aspect that truly is a part of the original concept of Moore's law is the component element. The evaluations of Moore's law show that we must continue moving forward in addressing the intricacies involved in our technological

environments as to the eventual consequences that could befall the global environment, given the magnitude of the scope provided, and the future evaluations of the morphism and adaptation of technological environments, as depicted by DeBenedictis (2017).

Technologies are evolving in ways that are difficult to predict. Cusumano and Yoffie (2016) explored elements for moving forward in addressing newer technologies, in that Moore's law was a foundational impetus for major companies, such as Intel, Microsoft, and Apple, which provided a forecast that has held true over the years. What will the future hold after Moore's law, questioned Cusumano and Yoffie (2016), in relation to our assumptions of hardware, software, and digital advancements? These questions are fundamental and should be examined and answered using a multidisciplinary approach, including a wide array of participation among public and private sector subject matter experts and leaders (Cusumano & Yoffie, 2016).

Literature Review

We are entering an era of machine learning and virtual and augmented realities, which provides even further implications for policy development in the realm of privacy and security. Proactive international policy development, in the realm of virtual technologies, and a continuous multidisciplinary approach for immediately addressing security issues along the way will help provide some continuity for helping to protect our global societies from the technological threat landscape that has proliferated, practically unnoticed, over the past several decades. The following concepts, consisting of the threat landscape of cybercrime in relation to criminal hacking, privacy and security issues in relation to criminal hacking, and policy and laws for the punishments of criminal hacking

have been examined with an overview of the hacking environment. All the elements of the study connect in various ways, as can be seen in the subsequent passages.

Threat Landscape

It was stated at the 2016 European Intelligence and Security Informatics Conference, as cited in (Choo, 2008; Kshetri, 2010; Wall and Williams, 2013 &Yip, Webber, Shadbolt, 2013), "Security and intelligence agencies in the UK, the USA and Australia consider cybercrime one of the most critical threats today, putting it on the same level as global terrorism (Mikhaylov & Frank, 2016, p.80)." The cyber threat landscape continues to evolve with the growth of emerging technologies and the vast speed at which these technologies work.

When did the first discussions of cyber policies first take place? Warner (2012) clarified how the history of cybersecurity may be surprising to some in that the concern for securing our data and technologies started long before most had the opportunity of learning what security was about in the technology realm. Although there is not research depicting exactly when cyber policies were first contemplated by government officials, it was recognized at the government level, starting in the 1960's, four threats involving our technological advancements, which would eventually influence future policy in the cyber realm (Warner, 2012).

As early as the 1960s, explained Warner (2012), it was known, through the declassification of government documents, that sensitive data on computers could be leaked by computers and should be protected, as well it was realized in the 1970s that data could be stolen by attacks on computers. Military arsenals were discovered to be

able to house computer attacks in the 1980s through the 1990s and the realization that if we could accomplish computer attacks, then other countries may possess the same abilities (Warner, 2012). Warner (2012) continued, by showing statements made by Willis H. Ware, in 1967, at the Spring Joint Computer Conference on the 'Security and Privacy in Computer Systems' that vulnerabilities to computer systems included humans, hardware, software, and the organization of the system, all of which can contribute to the consequences of an intrusion, which makes whatever is housed on the system available to the intruder. It was also shown from the conference proceedings that looking to what could be achieved through vulnerabilities should also be considered (Warner, 2012).

The following report identified the need for addressing the problems we are dealing with today, with the vastness of the environment to be addressed. Warner (2012) showed how it was understood by officials in the 1970s, through a classified report from the RAND corporation, that there could be no security, through engineering, that would be able to protect the technologies of the day and any type of sensitive data should not be stored in the technological environment without excepting a profound risk of discovery, as cited in the (Report of the Defense Science Board Task force on Computer Security, Security Controls for Computer Systems, Ware Report, Feb.11, 1970, published by the Office of the Director of Defense Research). One can only imagine what our cyber realm would be like today if proactive security and policy measures were headed with expedited actions among our international communities from the onset.

History can offer many insights for present-day cybersecurity issues. The human propensity to commit crimes will continue to make up global environments, if the history

of the world, as it is known today, continues to hold true, stated Williams (2015), in that crimes of the past are crimes of the present, although committed using different methodologies or approaches. A look at history showed how in 1944 the Office of Strategic Services, put out a field manual entitled *Simple Sabotage Field Manual*, which detailed the motivating factors for recruiting citizens for the cause during World War II, including the personal benefits and sense of value and belonging (Williams, 2015). This historic insight furnishes a framework that could help in discovering the motivating factors behind the hacking mentality and whether these factors contribute to the criminal acts of hacking.

Industrial espionage is a very big problem equating to approximately $300 billion a year and growing, especially for international travelers and the loss of intellectual property in international hotel rooms (Benice, 2012). Methods such as covert room intrusions, which include physical entry to gain valuables, computer data copies, and accessing items in the room safe are typical ways that are used to gain intellectual property covertly and can provide information for potential blackmail (Benice, 2012). Room stacking, which uses corner rooms to place wiring on the exterior of each level, so it is not easily detected, provides for an additional method that is used to spy on international travelers in gaining proprietary information (Benice, 2012; Richmond, Morrison, & Covarrubias, 2017). These are only a few examples of what is taking place on the international scene in relation to industrial espionage but can also be evaluated in terms of individual privacy expectations (Richmond et al., 2017).

A recent study provided by the RAND Corporation showed how the cybercriminal markets are on the rise and can be more profitable than the drug trade, given the ease in which hacking tools can be obtained and the ability to use private anonymous networks, such as the dark net, for recruiting and business dealings (Ablon & Libicki, 2015). Virtual tools and the Internet's encryption provided a way for terrorist organizations to spread malware without being detected, further assisting them in accomplishing their ideological agendas (Gewirtz, 2016). Emergency communications are now vulnerable to being compromised by terrorists and hackers who aim to disrupt the system for gaining an advantage for their political or ideological goals, which holds several implications for security professionals in the quest to secure critical environments in the cases of emergency situations (Gewirtz, 2013).

Castelluccio (2017) elaborated on some of the infamous hacks during 2016, including smart home devices, bitcoin losing over $75 million, and a digital bank robbery taking approximately $81 million dollars of Bangladesh's money from the Federal Reserve Bank of New York, showing how profitable hacking attacks can be. The interconnectivity of our technological devices provided the opportunities for intrusions, especially through Wireless. It has been shown that children's toys are vulnerable to hacking, this was discovered when the kid connect services, through the Learning Lodge, was compromised and millions of data records were taken, including over 6 million records of children and a whole year of chatting communication records (*Wide Range of Devices Vulnerable to Hacking,* 2015). Our online schools are also vulnerable to the

risks of hacking, as shown from a study conducted on early E-learning systems (Mihai, Pruna, & Petrica, 2017).

Wireless Sensor Networks (WSN), stated Juliadotter *Hacking smart parking meters* (2016) from a study on how smart parking meters can be hacked, proved to be a virtual avenue vulnerable to intrusions and the methodologies and motivations behind these types of hacks can vary. The study found the impacts of a hack could include data compromise, the disruption of service, and false data produced by manipulating the network packets that could have many consequences in the disruption of service *(Hacking Smart Parking Meters,* 2016). It was found in categorizing the attack of a smart meter that the threat agents encompass motivations in the form of gaining data for nefarious purposes, for political purposes, or for not wanting to pay for parking a vehicle *(Hacking Smart Parking Meters,* 2016).

Autonomous vehicles have been developed and are being tested on roads today in the United States, which provides questions to the safety of the technologies being used. Jafarnejad et al. (2015) illustrated how there are security issues with connected vehicles through a car hacking experiment with the best of the best technologies imbedded into modern-day vehicles. The challenge concluded with many vulnerabilities that included the hacker being able to manipulate the car in moving forwards or backwards, manipulations with lowering the speed, and manipulating and changing data on the dashboard, to name a few (Jafarbehad et al., 2015). These penetration tests showed that a vehicle can be criminally hacked, providing for potentially serious security and safety implications (Jafarbehad et al., 2015; Wenzel, 2017).

A prototype quantum communications satellite, with a nickname of Micius, explained Castelluccio (2016), designed to make communications extremely secure through cryptology, was sent out by China in August of 2016. This showed how the technological virtual realm is vulnerable in space and there is a need for extra security, although this extra security could also provide a way for paths to be covered and not to be traceable or detectable when examining virtual crimes, due to the cryptographic elements, if this type of quantum technology is embraced by the criminal realm in the future. It has been discovered that a 3-D printer hooked up to the Internet provided an avenue for hacking to manipulate with the printer itself or specifically causing various defects to be present within the created model (*3D Printing is Vulnerable to Hackers, 2016*).

There are technological security breaches every day, explained Mansfield-Devine (2014), and the hacking incidents today are not on a small scale, they are industrial in scale to what has taken place in previous years. Banks are a major target for criminal hackers, due to the amount of money that can be exfiltrated (Mansfield-Devine, 2014). Not only do criminal hacking incidents aim to target organizations for financial reasons, hackers are joining forces to form what is termed a hacker collective, for purposes of nation state hacking for any given purpose or agenda, including espionage, terrorism, and electronic surveillance (Banks, 2017; Gerwirtz, 2011; Van DerWalt, 2017).

As-a-service, referring to hacking that is outsourced, stated Ablon and Liciki (2015), has grown substantially over the years and can be very profitable. An infamous Russian hacker, Peter Levashov, charged $500 for his services in sending phishing attacks through email, using a profitably set up botnet network, involving multiple

thousands of computers, that could be controlled remotely ($500, 2017). Peter Levashov was arrested in Spain on April 14, 2017 and the Kelihos network, of approximately 100,000 malware infected private computers, and was taken down *($500, 2017*).

Hacktivism is gaining momentum in our modern-day culture due to the transparency and availability of data that can be used to target groups or individuals (Gewirtz, 2011; Wood, 2015). The tools are readily available for these attacks, as well as any other types of hacking attacks (Juliadotter, 2016). Gewirtz (2015) illustrated how social media sites, including career related sites, are being used as an entry way into virtual attacks, especially those dealing with critical infrastructure for any given political cause. Illegal hacker activity in the cyber realm includes the Syrian civil war and the Syrian Electronic Army (SEA), stated Mansfield-Devine (2014), where denial of service attacks and social media account hijacking is common through the hacktivism mindset. Since 2011, the private sector security organization, FireEye, showed how the Syrian Malware Team initiates attacks through Remote Access Trojans (RAT), which aims to take data in espionage attempts, having far more consequences than the activities of the SEA.

Online social networks have proven to be a huge vector for online criminal activity in the realm of black hat hackers and their recruitment of followers, as well as with terrorist organizations and the recruitment of individuals for their cause (Al-khateeb, Conlan, Agarwal1, Baggili, & Breitinger, 2016). Al-khateeb et al. (2016) continued to show how these social media networks, vulnerable to criminal hacker networks and terrorist organizations, has been taking place since the inception of online social

networks. Tracing of communications for the recruitment activities of these groups has proven to be very difficult to ascertain through the digital forensic methods and tools used by many today, due to the amount of big data elements involved within the online social networks (Al-khateeb et al., 2016).

Criminal hacking, in its various forms, is a global problem and continues to be a major part of the cyber threat landscape. Burkart and McCourt (2017) detailed how software packages designed to target individuals and various entities, for gaining all types of information, is being purchased on a global scale within the confounds of the law, since there is little regulatory deterrence outside of the regulatory frameworks put in place for intellectual property rights. This growing phenomenon of cybersecurity software, developed for addressing the need for offensive and defensive cybersecurity methods in securing our networks and technologies, provides tools that can be used for nefarious purposes, and has given rise to a political international economy of vendors and clients capable of providing many types of surveillances (Burkhart & McCourt, 2017).

Artificial Intelligence (AI) and machine learning (ML) have accelerated to the point today were the technologies are being used to increase productivity and efficiency on a number of legal fronts. On the other hand, Solomon (2020) illustrated how AI and ML are being used as tools to help hackers in advancing their agenda's for finding vulnerabilities in systems and for creating high quality phishing campaigns in their attempts to targeting influential individuals. The use of AI in the wrong hands is one of the newer emerging threats, among the multitudes, in the threat landscape of criminal hacking.

Hacking

The terminology of hacking has been around for decades, depicting activities that can be ethical or criminal. The methods used for hacking commonly consist of using readily available tools or programs for penetrating technological devices. One form of hacking is ethical hacking, which is used by many organizations and businesses in the public and private sectors in testing for security vulnerabilities. Ethical hacking is gaining in popularity all over the world in academia and for red and blue team competitions, where a secured environment is used to test security vulnerabilities and for gaining experience in the penetration testing environment. Hacking tools are readily available, as well as hacking techniques are provided on the Internet through YouTube videos and various forums, as well as through academic books and journals.

The acts of criminal hacking can be difficult to define, in that practically any type of cybercrime could include the criminal acts of computer intrusion. Rashkovski, Naumovskil, and Naumovskil (2016) expounded on the elements that define hacking, as cited from (McQuade 2006;Taylor 1999), "… The standard broad definition of hacking encompasses all forms of using technology for purposes for which that technology is not intended" (Rashkovski et al., 2016, p.138). There are not universally accepted definitions for the acts of criminal hacking, as posited by the cybersecurity community and law enforcement officials, although definitions are put forth in some of the legislations internationally, all with some intricate variances. Rashkoski et al. (2016) continued, as cited by (McQuade 2006), "illegally gaining access to one or more computer systems by abusing the security shortcomings and overcoming the security obstacles such as

passwords and firewalls in order to use or steal data or to insert new (external) program functions" (Rashkoski et al., 2016, p. 139). "Under the CFAA, unauthorized access to a protected computer is punishable by a fine or by imprisonment" (Schultze, 2016, p.245).

Lipoff (*Hacking the house,* 2016, Ch. 1) illustrated how approximately 45 years ago, in the 70's when hacking involved telephone networks, he hacked the doorbell to his apartment to allow for his newspaper to be delivered through the locked lobby doors at the timing he specified, enabling for his newspaper to be delivered to his apartment door. Since then he has enhanced his methodologies for hacking his house, providing for technological conveniences for controlling various intricacies between the two homes he owns, which are separated by a five-hour airplane flight, seemingly being present at either location at the same time, due to cameras, lighting, and other technological illusions and manipulations (*Hacking the house,* 2016, Ch. 2-3).

Numerous computer intrusion tools have been developed over the last couple of decades and are commonly used to accomplish the tasks of criminal hacking. Juliadottter (2016) explained how the threat vectors, or the tools in this case, help in capturing Wi-Fi traffic, enabling for the intrusion into a smart parking meter. A couple of the tools used for this attack, other than a laptop with a wireless antenna, are *aircrack-ng* suite and *wireshark*, which can be used for the entire process (Juliadotter, 2016). These tools are readily available to acquire and are not only used by those committing computer crimes, but they are also used by public and private sector entities for security purposes and in virtual environments for the learning of ethical hacking techniques (Hausken, K. (2017).

Bradbury (2011) detailed a step by step methodology for cracking a network by scanning the environment to find vulnerabilities using various methods and penetration testing tools. Gold (2012) described how hacking can be done with a cell phone just as easy, if not more so, than with a laptop due to the advancements of software applications. Wireless computer intrusions can be accomplished in any given public area without being easily detected. These computer intrusion mobile apps can be used for ethical and criminal hacking purposes (Gold, 2012).

An empirical study, conducted by Bento and Bento (2014), consisted of 60 months of statistical data, on a hacking model, displayed various activities encompassing attacks through hacking. The model represented the following steps or variables, (reconnaissance, malicious code, user compromise, root compromise, and denial of service), as well as "two other variables that might have an impact on the growth of in security breaches: number of hosts in the Internet, and broadband access to the Internet by home and small business users" (Bento & Bento, 2014, p. 681).

The study found; "Reconnaissance (Step 1) is positively related to Malicious Code (the preferred route to achieve initial access in Step 2), supporting the model's prediction that increased efforts to find vulnerable systems are associated with increased attempts to break into them" (Bento & Bento, 2014, p 687). The study also found "Success in achieving User Compromise in Step 2 is positively related to Root Compromise (Step 3), which is compatible with hackers' attempts toward escalation of privilege." (Bento & Bento, 2014, p. 687) The final findings showed "…a negative relationship between Root Compromise and Denial of Service supports the idea that a

hacker's frustration at failing to gain control of a resource may be associated with trying to sabotage it through DoS attacks" (Bento & Bento, 2014, 268).

Hacking, as noted by many, is an inquisitive quest. If hacking is examined from a democracy viewpoint of having the ability to learn and become the best an individual can be in a free environment, it can be seen how those interested in the technological interworking's of the technological landscape may have great motivational aptitude to explore the intricacies of the field to personally excel in the quest for new knowledge, while gaining a sense of power (Hunsinger & Schrock, 2016). Soderberg and Delfanti (2015) extrapolated "…technical innovations spawned by hackers (modular software code, mesh computer networks, distributed retrieval systems, private cryptography, etc.) constitute the material infrastructure of today's capitalism" (p.795).

Human curiosity traits are a part of human nature. As cited in (Oudshoorn & Pinch 2005), "Hacking can be seen as a special case of a broader trend of citizen engagement with science and user appropriation of technology" (Söderberg & Delfanti, 2015, p.794). There were no policies in place to discourage or deter the activities of learning the intricacies of technology through hacking back when virtual hardware and software were first developed. When and where did the landscape change to that of those being on a quest to gain knowledge to that of exploiting technologies for personal gain, at the expense of anybody or anything that might be in the way?

Denning (1983), a contributor to the Association for Computing Machinery (AMC), posed questions, approximately 35 years ago, dealing with morality and clarity of trespassing in the digital age. The question of trespassing in the virtual realm was hard

to answer back then, stated Denning (1983), and the question is still trying to be answered today, with all of the intertwining intricacies. More than 60 businesses were reportedly broken into by a Milwaukee hacking club called "414 hackers", which one member was indicted for breaching the computers that held PII of cancer patients at Sloan-Kettering (Denning, 1983). Denning (1983) analogized how computer intrusions, like physical home invasions, physically accessing office filing cabinets, or somebody stealing your automobile without your permission or knowledge.

Societies are dealing with the same issues today, but on a significantly larger scale. It is hard to say how the hacking community has grown and proliferated throughout the years. Computer intrusions have gained in notoriety, "2014 was the year the hack went viral" (Ablon & Libicki, 2015, p. 143). How many hackers and/or groups exist today among international communities? Is it possible to change a culture that has evolved into what encompasses some aspects of all cultures today? The questions of the study aimed to provide insight, as to what is perceived by stakeholders in today's cybersecurity realm, for the way in which we should proceed forward in the legislative realm (Tang, Bagchi, & Jain, 2009).

Hacking in relation to privacy in the digital era has become a concern for many. Interestingly, a reporter for the Surfacing column (Hiltner, 2018), showed how some anonymity and privacy perceptions are moving in a different direction in the hacking realm from what was once considered to be the norm of only using aliases, which can be seen through interactions from hacker conferences, such as the annual hacking conference held in Las Vegas, Nevada, Defcon. Hiltner illustrated how the pressures

involving demands by the private and public sectors for experts in the cybersecurity field and bug bounty programs, propelled by professional entities and the gamification arena, have shown a present day need for various aspects of the hacking culture (Hiltner, 2018).

Trust among hackers has been studied with interesting results. Dupont, Côté, Savine, and Décary-Hétu, (2016) provided results of a mixed methods study, which analyzed trust among hackers in the hacking community, through examining approximately 30,000 respondents "belonging to the largest computer hacking forum" (Dupont et al., 2016, p.129). Findings from the analyzation of 449,478 collected feedbacks, over a 27-month period, from a random qualitative examination of 25,000 feedbacks "…that a diverse set of behaviors, skills and attitudes trigger assessments of trustworthiness" (Dupont et al., 2016).

What is portrayed in the news media on hacking should not be assumed to be reality. Donner (2016) explored the gender gap of college students and cybercrime and found that the male gender committed more online offenses in all categories studied, including self-control and the amount of time spent in the virtual environment. The quantitative study also found that both genders where equal in committing hacking and digital piracy offenses, when Internet usage was high (Donner, 2016). The results of the study found to be contrary to what is being reported in the media and journalist accounts, while providing valuable "…insights into the complex mix of transactional, behavioral, and cultural factors that establish someone's trustworthiness" (Dupont et al. 2016, p.131).

Numerous elements contribute to the hacking culture. Reinis (2016) conducted a worldwide study on the role of the environment encompassing an adolescent's life, such

as school, family, and the neighborhood one lives to see if these elements played any role in the propensity to commit cybercrimes, specifically in the realm of hacking and illegal downloads. The study involved 68,507 students from 30 countries and found "…parental control, attachment to family, self-control, attitudes toward violence, attachment and disorganization to school, and attachment, integration and disorganization of the neighborhood as possible predictors of illegal downloading and hacking" (Reinis, 2016, p.127). Other studies have been conducted, by experts in the field, on criminal hacking behaviors and motivations (Chua and Holt, 2016; Young & Zhang, 2007; Bachmann, M. (2010).

Motivational drive has been examined in many types of criminal cases in the criminal justice field. Mansfield-Devine (2014) interviewed Amichai Shulman, who stated we must look at the motivations behind the cybercriminal's actions, understanding why and how crimes are committed and who the targets are so it can be determined if there are criminal or political motivations involved, or if both are motivating factors. It is challenging to identify what the true motivations are behind various attacks, although politically speaking there are tremendous advancements being made in offensive types of attacks, showing the "industrialization of hacking" (Mansfield-Devine, 2014, p.14). "Technologies sold by companies like Gamma Group and Hacking Team create cross-border fact patterns that can seem more complex than traditional physical-world attacks" (Schultze, 2016, p. 895).

Similarly, motivation plays a pivotal role in understanding different cultures and the tendencies for hacking. Turgeman-Goldschmidt (2008) interviewed 54 Israeli

hackers and found their motivations and perceptions of who they are was instilled in them when they were young and no matter what the consequences are for hacking, it does not provide a deterrent for the acts of hacking. An interesting concept was found through a study on hackers' motivations, showing "Hackers appear to be more motivated by what they dislike rather than by what they value" (Madarie, 2017, p. 78). Cultural values global may pose a number of challenges when addressing multinational policy initiatives.

Privacy and Security

Security and privacy are fundamental today given the virtual landscape and it is expected that individuals are afforded these assumed rights either by what is legislated or through ethical assumptions (Greengard, 2012). Hooker and Pill (2016) showed how the legal arena is facing tremendous issues and is on target for major policy change over the years. A privacy case involving many data breaches with the Wyndham hotel group established that the privacy breaches of consumer PII data were verifiable under the Federal Trade Commission Act (Hooker & Pill, 2016). Privacy will be even more of an issue with the proliferation of big data and the continuous increase of data compromise in all virtual environments with connected devices, especially in the realm of the IoT, which opens increasing risks for an individual's privacy (Lindqvist & Neumann, 2017; Riga, 2017).

Data breaches are occurring on a regular basis, with the amount of comprised data being reported in the billions according to recent reports, from 2005 through August 13, 2017 there were 7,798 data breaches compromising the data of 904,769,967 records (*The Identity Theft Resource Center*). Din (2015) delineated between criminal breaches and

data scraping and determined there should be additional laws put in place to better distinguish between ethical and non-ethical data scraping, which should be criminalized as a data breach through robust anti-hacking legislation. The compromised data being collected through data scraping has privacy and security implications in our modern-day society more than ever before. Security practitioners and privacy advocates will need to help in the multidisciplinary approach of defining the security implications and helping in developing policies to address the escalating problem of data hacking (Din, 2015).

Stone (2012) demonstrated, due to the present-day threat landscape, political campaigns should consider keeping important information out of the virtual environment, to help ensure there are no breaches that could have an impact on the efforts that have been put forth toward any given election process. Considering the United States electoral process being hacked prior to the final presidential election in 2016, Shackelford et al. (2017) provided a study involving India, Germany, South Africa, Brazil, Estonia, and the United States on how their election processes are secured. The study showed how voting systems are vulnerable in many ways, depending on the systems being used and could potentially alter the course of democracies around the world if voting outcomes were compromised (Shackleford et al., 2017).

Certified public accounting (CPA) firms are buckling down to meet best standard practice goals for protecting their customer's data, in efforts to mitigate the risks of criminal hackers, due to requirements from the regulatory realm (Lanz & Cohen, 2012). The banking industry is working to speed up managing and mitigating risks in the financial sector, to help ensure the privacy of customer's data and PII (Mendelson, D., &

Mendelson, 2017). Today banks are being breached not only for monetary gain, but for the sensitive information that can be obtained for other purposes, such as for political means (Mansfield-Devine, 2014).

Gupta and Mata-Toledo (2016) showed how computer intrusions can cause irreparable damage to an individual through the access of personal information, likened to somebody having a full x-ray of your body with all the intricacies found within. There are grave consequences, in the legislation realm, for committing a physical assault on a person, which can be likened to what happens in some cases when personal data is exposed, it is like a vertical weapon of assault (Gupta & Mata-Toledo, 2016). From another perspective Snell (2016) elucidated that the more transparent our virtual world becomes, the more uncomfortable those that choose to lie and cheat will be, due to technologies encompassing practically every aspect of our daily lives, and the amount of data that is captured and preserved.

A number of critical infrastructures that countries rely heavily on for keeping information private are vulnerable to hacking. In medicine, personal information can be obtained or compromised through wireless hacking, as cited in (Denning et al., 2009) of brain computer interface (BCI) technologies, which showed ethical, security, and legal implications in relation to privacy (Ienca & Haselager, 2016). Stone (2012) demonstrated political campaigns should consider keeping important information out of the virtual environment, to help ensure there are no breaches that could have an impact on the efforts that have been put forth toward any given election process. Mansfield-Devine (2014) showed how advanced persistent threat attacks, from military groups in China, according

to a private sector organization, Mandiant, and various groups of the like, are responsible for the loss of PII of hospital patient records that accounted for patient data loss of 4.5 million records. PR Newswire (2017) reported that most law firms in the United States are not knowledgeable to the threats they are vulnerable to and the number of times their systems have been compromised by hackers in 2016, according to a Logic Force survey involving 200 law firms.

The tools used for technical intrusions are available on many fronts throughout the world, including retail markets. Burkart and McCourt (2017) described how there are security and privacy concerns with packaged software that is being developed and distributed, in markets that have minimal regulation in the technological realm, for the purposes of online surveillance. The European Union addressed, through policy, the protection of personally identifiable information in the form of a framework, which regulates marketing of PII (Burkart & McCourt, 2017). This type of framework has not been implemented in the United States, although there is hope for these issues to be addressed through self-regulation in industry, which could potentially help in the implementation of international treaties addressing the trade in these markets for curtailing various security and privacy concerns, stated Burkart and McCourt (2017).

According to a Canadian expert Michele Mosca with the University of Waterloo's Institute for Quantum Computing, Co-founder and Program Director, stated Solomon (Encryption breaking quantum computers getting closer, warns Canadian expert, 2017), it is estimated that the RSA 2048 encryption could be broken within the next ten years, if the one in seven chances estimate holds true from the Quantum Safe Workshop held in

Toronto. The odds have now moved to a one in six chances, according to Mosca, and the "quantum computer will break the way we do cyber security, the way we do crypto (graphy) today, and we need to solve it" (as cited from Solomon in Encryption breaking quantum computers getting closer, warns Canadian expert, 2017). Encryption today not only helps secure our critical infrastructures, while providing privacy to individuals and enterprises, it also provides a means for criminals to proceed with their criminal activities without being detected (*The Day the Cryptography Dies*, 2017). Proactive coordinative efforts should be taken to help ensure societies can continue with the encryption technology that provides security in the virtual realm, while addressing the protection it provides to the criminal element (*The Day the Cryptography Dies*, 2017).

Many security professionals have found that human error contributes a great deal to security compromise. The human element in computer security is the weakest element, explained Brink (*10 Questions with Derek Brink*, 2003), while passwords have continued to present a problem in the virtual realm, an awareness approach to addressing the vulnerability of the human element can provide for improvements in moving forward in analyzing cybersecurity issues until there is a population that is mostly technological savvy given due to their experiences from inception. "Technology is flawed, networks are porous, and all of it is powered by error-prone humans" (Williams, 2017, p. 6).

Those committing virtual crimes can inflict a number of abuses on individuals, businesses, organizations, government entities, and nation states, to name a few. Wilsem (2013) described the connections between hacking and harassment and how the psychological effects produced from the technological harassment, are like those

produced from violence crimes, but with more far reaching consequences, such as with the hacking of personal information that can be used to destroy the reputation of an entity or an individual. These types of crimes will grow and the technological landscape continues to proliferate. Policy development should consider the lasting damages computer-focused and computer- assisted crimes cause the individual and/or the entities involved.

The future should offer improvements in cybersecurity, in that the populations will have grown up with technological devices, providing for a population with a better understanding toward addressing technological issues (Ablon & Lubicki, 2016). With there being a total of 195 sovereign states around the world, global societies must continue to take a defensive stance with cyber intrusions until legislative bodies draft rules, and enforcement strategies for those rules, that will address all computer intrusion crimes (Williams, 2017). Kosseff (2017) illustrated how the standards for privacy from the European Commission have set the course as the highest of standards and have stated that jurisdictions from the following countries have measured "to be adequate: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay (Kosseff, 2017, Chapter 10).

Policy and Law

Government policy making has been noted by many to be slow, rather than expedient, when tackling issues that need to be addressed in the policy realm, in general. Sabett (2016) compared Moore's law with the legislation implementation showing how some laws in the United States are outdated by the time they are implemented as with the

Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA), although Moore's law has stood the test of time and proven its predictability. To effectively prosecute crimes using the ECPA and the CFAA there needs to be a very good understanding of how security works in the cyber realm (Sabett, 2016). This where a multidisciplinary approach comprising of subject matter experts may be beneficial in addressing ongoing multinational coordinative legislation initiatives.

Cyber policy legislation has gained attention over the years with the evolving nature of technologies. The United States National Security Act of 1947 and the Computer Fraud and Abuse Act of 1986 predates the terminology of cybersecurity law, although these Acts have been revised since then, valuable insights can be gained from revisiting and closely examining documents of the past for establishing future policies (Williams, 2015). The United States held many hearings starting in 1985 to accomplish what was later legislated as the Computer Security Act of 1987, which allowed for the National Security Agency to protect networks in relation to national security and for the National Bureau of Standards to protect networks in relation to federal entities, other than the Department of Defense (Warner, 2012).

History has shown, expressed Warner (2012), the time in which it has taken for successfully addressing the cybersecurity issues of today, given U.S. government officials were being briefed in the 1960s. The difficulty is addressing these technological issues was overwhelming at the time for, "…for any one agency or department to solve on its own, and too complicated for the White House and Capitol Hill to solve with any single bill or edict" (Warner, 2012, p.799). The time element will continue to pose

challenges in the legislative realm given the speed at which newer technologies are being developed.

In February of 2016 the Cybersecurity National Action Plan (CNAP) was revealed in the by the U.S. government providing a framework in dealing with today's computer intrusions, stated which included "enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security (as cited from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan)" stated Sabett (2017). The Cybersecurity Information Sharing Act (CISA) was released in 2016 providing for voluntarily sharing information, in relation to cybersecurity, without having to fear legal repercussions (Sabett, 2017).

On June 6, 2016, the Boston Global Forum announced, "Leaders at the G7 Summit approved the first international stand-alone agreement on cybersecurity, including data protection and Internet governance" (http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/)" The group of 7 (G7), the United Kingdom, Germany, France, the United States, Canada, Japan, and Italy, have been working to establish common ground for addressing human rights issues in relation to the cyber realm, which includes privacy and the continuation of information and communication technology freedoms (Shackleford, 2017, a). Shackleford (2017a) continued to show how there is a need for coordinative efforts toward "verification, transparency, and extraterritoriality in the sustainable due diligence context comprising cybersecurity, data privacy, and human rights

considerations" (Shackleford, 2017a, pp.884-885). Shackleford (2017a) further illustrated what the consequences would be if we choose not to address issues of due diligence in cybersecurity, in that we will be facing, as cited from (*Bendiek, supra note* 75, at 32) a "collision course for different national legal systems, which would encourage the fragmentation of the global economic space and the Internet" (Shackleford, 2017a, p. 885).

Shackleford et al. (2017) illustrated how some countries are developing policies and legislation to address the cyber vulnerabilities of their critical infrastructures. In the context of the election processes around the world, which could be appropriated as critical infrastructures, information sharing among international bodies and a physical paper audit trail of every individual vote, provides a couple of elements that can be addressed in the electoral processes for helping to mitigate the inherent risks involved in voting processes, while improving the election infrastructures around the world (Shackleford et al., 2017). McMillan (2009) showed how, just prior to China's strengthened cyber laws, some professionals in IT chose to take the crime route during a time of economic struggle in china. An approach of broadening the definition of cybercrime and extending the penalties to fit the "tremendous social harm" (as from McMillian, 2009, p. 74) has been taken to help mitigate the virtual crimes the world is facing today.

International law considers universal jurisdiction, which provides nation state courts the ability to hold criminal actors accountable for their crimes through prosecution, although recent legislations have prompted for more stringent guidelines for addressing

the intricacies involved in universal jurisdiction prosecutions and international relations (International Law - Universal Jurisdiction - United Kingdom Adds Barrier to Private Prosecution of Universal Jurisdiction Crimes, 2012). An example can be seen through The United Kingdom Police Reform and Social Responsibility Act of 2011, which has made it more difficult for universal jurisdiction cases to work in some cases given a new requirement of "consent of the U.K. Director of Public Prosecutions before a U.K. court can issue a privately sought arrest warrant for universal jurisdiction offenses. The requirement separates universal jurisdiction crimes from the arrest warrant procedures for domestic crimes in the United Kingdom" (International Law - Universal Jurisdiction - United Kingdom Adds Barrier to Private Prosecution of Universal Jurisdiction Crimes, 2012).

A new approach for addressing the governance problems in securing our information, proposed Elkin-Korerd and Haber (2016), showed how a nonbiased oversight body could provide the needed insight on how information is used in the ever-increasing world of transparency, rather than trying to track down how the information was procured. For civilian liberties and global security to be equally addressed, online intermediaries and public-private partnerships, along with an oversight body providing a proxy for governance, would allow governmental agencies the needed information from networks and distributed networks for addressing criminal acts without overstepping the boundaries of civil liberties (Elkin-Korerd & Haber, 2016).

Trotta (2017) explained how a mixture of expert technocrat knowledge, coupled with the knowledge of the citizenry, enhances the policy making process for legislators

by helping to ensure policy solutions are brought to the table. Visher and Weisburd (1998) showed how there needs to be tailored approaches for crime prevention strategies, to help ensure recidivism rates decrease and are potentially alleviated. These approaches should involve concerted efforts among stakeholders in establishing and implementing unique programs with precise elements for addressing a specific type of crime (Visher & Weisburd, 1998).

The General Data and Privacy Regulation (GDPR), put into full force on May 25, 2018, provides strict penalties for companies not adhering to the regulation in the EU, as well as for companies that do business with the EU abroad. Goddard (2017), Director of policy and Standards, MRS, and Director of Policy and Communications for EFAMRO, states "GDPR goes beyond current law in demanding higher standards for organisations processing data – but these higher standards are philosophically in line with best practice and ethical approaches that are practiced by research practitioners" Goddard (2017) goes on to state, "GDPR builds on transparency and trust enshrined in national and international codes with best practices that put the interests of research participants rightfully at the center" (2017, p. 705).

The 2014 Sony breach provided an example of how international law has not been able to address nation state cyber-attacks, according to many expert legal examinations of the international law, for assigning criminal culpability for the actions taken by North Korea in response to a scheduled release of the movie *The Interview* (Shackelford, 2017b; Sullivan, 2015; & Walton, 2017). Contrary to some scholarly thoughts and proposals of international frameworks for addressing cyberspace attacks through international law and

treaties, Walton (2017, p. 1460) suggested a liability and duty centered approach, which would specifically address "low intensity" destructive cyber-attacks that fall outside of what is currently addressed and understood by many under international law. This approach "that derives from a preexisting but underutilized source of international law: liability for transboundary harm" (Walton, 2017, p.1464), would use the "harm" element in relation to a low-intensity cyber-attacks from any nation state, with a special focus on the responsibilities of the state, providing for consideration for the acts to be criminal through international law (Walton, 2017).

Existing laws and treaties can be used to address our current cybersecurity issues stated Shackelford (2017b), we can look at "…how the public law of cyber peace may be combined with private international law to create the legal foundation for a global culture of cybersecurity (Shackelford, 2017b, p.9) 1st article." The International Telecommunication Union treaty has been used, along with bilateral and multilateral treaties related to investments and trade, to provide a case for prosecuting private entities for cyber-attacks internationally (Shackelford, 2017b). Shackelford (2017b) showed how G20 has been instrumental in promoting the law of cyber peace internationally by examining the conduct of nation states in the virtual realm, including the acts of espionage and critical infrastructure protection in a holistic collaborative forum.

Considering the role each nation plays for responsibly addressing the security of the citizenry and the efforts put forth by normative powers in promoting a modicum of peace throughout conflict stricken global societies, Bengtsson and Elgstrom (2012) illustrated how the EU exemplifies a normative power, in relation to role theory, in

showing what is expected from the EU in helping to provide solutions for international issues in the realm of international relations. Although, the role of the EU is sometimes perceived in conflict to what is expected from the national actor in the context of role theory and how it plays out on the international scene, the EU is positively setting the stage for additional nation states to come on the scene in their modern-day attempts in accepting and implementing a democracy landscape on some fronts (Bengtsson & Elgstrom, 2012).

The role of international leaders will be instrumental in propelling change in the cyber policy realm. Abigbuo (2007) stated, as cited from (Holsti, 1970), how role theory provides a fundamental impetus for contributing to foreign policy efforts and positively adding to the models of International Relations (IR) theories, including how multidisciplinary leaders perceive their role on the political scene and what is expected in relation to their participation. Role theory in foreign policy, illustrated Adigbuo (2007), as cited from (Adigbuo, 2005; LePrestre, 1997), encompasses concepts of any of the following elements; behaviors that are expected, the rank of any given participatory individual, or the acts of an influencer or contributor. Role theory, with its multidisciplinary approach, provides a positive focus for moving forward with how Nigeria will define its role among national leaders for dealing with policy issues (Adigbuo, 2007).

International cooperation efforts have been underway on several fronts, as reported in the Economic Co-Operation and Development (OECD) 2017 Secretary-Generals' Report to Ministers, in working with stakeholders in addressing global issues,

since the inception of the OECD over 50 years ago. Working multilaterally with the cooperation of a wide array of stakeholders, including Public Private Partnerships (PPP), to address the issues relating to the present-day technological landscape and emerging technology issues (Secretary-Generals' Report to Ministers, OECD, 2017). The Strategic Orientations of the Secretary-General, Meeting of the OECD Council at the Ministerial Level, in June 2017 provided a strategic framework overview for establishing improved policies and multilateral cooperation and insights for the wellbeing of global communities, examining exclusion obstacles, and the use of metrics for driving better decision making processes, among the international collective body of 35 countries, for strengthening multilateral cooperation efforts toward addressing global issues and establishing international policies.

International coordinated efforts have continued toward an international consensus on some fronts, as touched upon in chapter 1. While there are international initiatives underway to secure the cyber realm, including strategies being developed to address the intricacies involved in cyber-criminal activities, confusion exists on how the global community should proceed forward in confronting the problems the world is facing today in cyberspace (Weber & Studer, 2016). There continues to be a gap in internationally developed and adopted policy frameworks for addressing today's cybercrimes and our virtual security (Weber & Studer, 2016). Upol (2014) explained how the Group of Eight organization became the Group of Seven after Russia was not invited back due to their involvement in the Ukraine crisis and Russia taking Crimea. It was reported "…the G7 leaders issued a statement saying, 'international law prohibits the

acquisition of part or all of another state's territory through coercion or force" (Upol, 2014, para. 1).

Garris (2017) illustrated the need for a collaboration of international entities for capturing major cybercrime organizations. As cited from (Germano, 2014), public and private partnerships are essential for addressing cyber threats but there is a need to overcome the obstacles that are preventing fruition of these partnerships, which include control issues in relation to incident response, liability in the evolutionary regulatory realm, cross border criminal investigations, and disclosure issues (Garris, 2017). In the United States, elaborated Schultze (2016), technological crimes can be prosecuted without the creation of new laws by using the intricacies of established legislations that were originally implemented for addressing traditional crimes, such as The Wiretap Act, which addresses intrusive technologies, such as spyware, and The Foreign Sovereign Immunity Act (FISA), which recognizes various exceptions to immunity. "Under the CFAA, unauthorized access to a protected computer is punishable by a fine or by imprisonment" (Schultze, 2016, p.245).

Work has been accomplished on a number of fronts in addressing criminal hacking. According to Kosseff (2017) various laws in the United States are used to help authorities in prosecuting the crimes of criminal hacking. The following are laws that have helped in bringing counts of violations against various entities, including single count violations, which carry prison sentences of approximately 10 years or more.

- The Computer Fraud and Abuse Act
- State Computer Hacking Laws

- Section 1201 of the Digital Millennium Copyright Act
- Economic Espionage Act
- Stored Communication Act (section 2701)

Kosseff (2017) continued to elaborate how some nations have done more than the U.S. in providing a legal framework for regulating data security and privacy. The following five countries, which are the largest counties for U.S. trading, have established regulations for addressing cybersecurity: European Union implemented the General Data Protection Regulation (GDPR) that updated their 1995 privacy law, Canada uses the Personal Information and Electronic Documents Act (PIPEDA) as their primary data security and privacy law, China uses the Consumer Protection Law, Mexico uses eight principals, which requires consent through various methods for undeniable clarity, and Japan mostly uses the Act on the Protection of Personal Information (APPI) to govern their data security and privacy (Kosseff, 2017).

There is a good deal of work ahead in policy making for determining all the variables that make up criminal hacking, including the various methods used in the exploits. Victimization of hacking is an area with little research, although it should be fundamentally considered when approaching the policies that are established for punishing the offenses of criminal hacking, elucidated Wilsem (2013). There is the need for additional research in the motivating factors behind victimizing through hacking and/or malware infections, to establish more effective policies for computer intrusions, whether they are computer focused crimes or computer assisted crimes (Wilsem, 2013).

Rashkovski et al. (2016) displayed how the Republic of Macedonia has been affected by punishable cybercrimes, which includes those that have been identified in relation to information and communication technologies that encompass the networks of the Internet, computers and connected devices, and mobile devices. The Republic of Macedonia has the least in numbers of Internet users, according to Rashkovski et al. (2016) study, but ranked second, after the United States, in the number of crimes reported. Although the Republic of Macedonia's legislative realm is moving forward addressing cybercrime, with the best standards in motion today throughout the world, Rashkovski et al. (2016) explained there is more needed to help in the global efforts, by including the authorities of Macedonia in global efforts toward finding solutions for adverting the criminal activities and enforcing more stringent strategies in addressing and mitigating the effects of cybercrime.

Pun (2017) described cyber espionage as being like the Cold War espionage with aircraft spying activities, where "…malware deployed can be changed on-the-fly to achieve a destructive capacity rather than mere surveillance (and often does so to wipe its traces from the hardware). For the victim state in both cases, there is fear the vehicle is intended for combat rather than surveillance" (2017, p.375). On Sept. 25, 2015 it was revealed that the United States and China had come to an agreement that each country would not steal trade secrets and would put forth concerted efforts to help ensure trade and economic proprietary information is not gained through cyber theft (*The Latest: US, China Agree Not to Steal Trade Secrets*, 2015). More recently Kennedy and Xiaoyan (2017) stated China just past cybersecurity law.

Many of the same hacking tools and techniques used by law enforcement entities are being used by criminals (Sommer, 2006). A study proposed a policy approach for the criminalization of computer intrusion tools, although it was noted there would be an impact felt in the areas outside of law enforcement, including those entities that use penetration tools in the academic environment and for ethical business purposes (Sommer, 2006). Ghappour (2017) pointed out how a standard framework needs to be adopted to help ensure there is consistency in the practices of cross-border investigation, which will play an important role in the policy environment for establishing and reaching a uniform framework for the crimes of criminal hacking (Hui, Kim, & Wang, 2017).

Criminal hacking investigations can be investigated and speedily addressed legislatively through various international assistance channels. These channels involve using informal cooperation methods of business to business investigative contacts, in the public or private sectors, or through formal cooperation methods, which involve a more in-depth approach of working with national governments and may require mutual legal assistance through a treaty, which is required for any type of digital evidence transfers relating to interception of communications and search and seizures (How Businesses Can Speed up International Cybercrime Investigations, 2017). Newer approaches, in addressing rulemaking and policies holistically, on a global scale, in the cyber realm could offer even more investigative efficiencies for the future.

"The individual-agent approach to prosecuting hackers recently bore its first fruit. On March 22, 2016 in the United States v. Su Bin, a Chinese businessman living in Canada agreed to plead guilty to criminal violations of the computer Fraud and Abuse

Act… "(Schultze, 2016 p. 245). This espionage hacking incident was criminalized for compromising Boeing, a United States aircraft company, servers and stealing trade secrets (Schultze, 2016). Although initiatives have been underway in addressing cybercrime, stated Greengard (2012), China and Russia are not represented in one of the more prominent initiative of the Council of Europe's Convention on Cybercrime. With no global policy in sight for addressing cybercrime, we have much to work on, including the "increasing continuous battle over rights, responsibilities, and resources" (Greengard, 2012).

The Black Report, a study involving a survey of professional penetration testers, hackers, and incident responders, led by Pogue (2018), addressed the hacking ability from the diverse population of 112 respondents. The study showed 34 percent of the respondents said they have been hacking 10 or more years and approximately 67 percent of the respondents said they spent more than 10 hours a week "bypassing IT security systems" (Progue, The Black Report, 2018, p. 9). Future studies may garner additional insights toward the number of individuals, among the global population, who have technical abilities and the skills required to hack into secured systems. These studies may offer various perspectives for the legislative realm in addressing how policies should be built, in relation to criminal hacking offenses, and what defines criminal hacking offenses, as a universal policy.

Hacking skills can be very valuable in today's virtual landscape environment, provided they are used in ethical ways. Various public and private sector entities have incorporated the skills of hackers, through crowdsourced programs, to help find

cybersecurity vulnerabilities in systems. The United States Air Force initiated a program that allowed hackers to hack Air Force systems in efforts to find vulnerabilities, and how this structured program has continued on to its third round of inviting hackers to hack the Air Force, through an invitation to 191 countries, for the opportunity to find vulnerabilities in a system recently moved to the virtual cloud (Cordell, 2018).

Although ethical hackers provide a great service in helping companies with their cybersecurity needs, new creative approaches are needed for addressing the intricacies associated with criminal hacking. Huang, Siegel, and Madnick (2018) illustrated crimes related to various hacking services and innovations have grown to several trillion dollars and are estimated to reach approximately six trillion over the next couple of years (as cited from Steve Morgan, 2016 – *Hackerpocalypse: A Cybercrime Revelation. Technical Report. Cybersecurity Ventures*. 1-24). With approximately one third of companies being touched by cybercrime, policies, outside of the realm of protection protocols, are needed to encourage additional proactive actions to help curtail the effectiveness of the cybercrime business (Huang et al., 2018).

There is need to holistically understand the hacking culture today in order to successfully address solutions to the problem of criminal hacking. A study, conducted by *Absolute Software Corporation*, found approximately one third of the IT personnel in the United States, surveyed admitted to hacking in their organization (2016, February 19). Additionally, the study showed among the information security practitioner respondents, that those between the ages of 18-44 were more apt to hack into their own organization (415 percent of respondents between the ages of 18-44) and those respondents 45 years of

age and older were less likely to hack into their own organization (12 percent of respondents aged 45 and older).

There are differing opinions on the types of policies that should be implemented for punishing the crimes of criminal hacking. In examining the disparities of penalties associated with various computer intrusion crimes, such as with hacktivism and Anonymous, Tomblin and Jenion (2016) argued that policy makers and sentencing imposed by justice systems around the world should be minimized in relation to recent trends of stricter punishments. A study conducted using age and crime, the curve showed most offenses lesson or desist as individuals age out of their teens and twenties, which offers valuable insight for policy makers in evaluating the effectiveness of deterrence methods (Tomblin & Jenion, 2016).

Summary and Conclusions

The major themes covered in the literature touch on various aspects of cybercrime, privacy, security, the hacking culture, and multinational policies and laws in the cybersecurity realm, which provided an in-depth look at the threat landscape of the technological realm for future policy considerations. The threat landscape, consisting of individual and group actors of criminal hacking, the methodologies and tools used to accomplish their missions, and the targets they aim to compromise, as illustrated by Weber and Studer (2016), should be understood holistically, with a team of subject matter experts for appropriately addressing a framework for international policy implementation for the criminal activities of hacking. The threat landscape encompasses a vast array of interconnected elements, including the political arena, industry, nation

state policies, cultural differences, and the propagation of the hacking community, all of which play some role, on the international scene, in relation to intrusions in the technological realm (Walden, 2004).

There is much to sift through when holistically addressing policies related to the acts of criminal hacking, and for consideration to be implemented at the international level. Those that commit the crimes, their methods, and their targets furnishes some of the elements needed for developing a framework for an international policy standard (Banks, 2017; Thaw, 2014). It is not known the extent in which criminal hacking takes place on a personal level through the various methods used for accessing all types of virtual technologies, although studies have shown, through private sector organization reports, that the number of network intrusions are continuously escalating.

The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for one international law for defining criminal hacking and the penalties associated with the act of criminal hacking. This study provided for extended knowledge to be gained in the cybersecurity realm, consisting of data contributions among multidisciplinary individuals on criminalization standards for the acts of technological intrusion crimes. The questions of the study furnished a foundation that was examined using descriptive and inferential statistics that provided the perceptions among individual stakeholders in the public and private sectors. An identification of differential standards for the definitions and punishments of criminal hacking were gained in hopes to help propel global awareness of the virtual threat landscape involving criminal hacking and to

promote international efforts for working in concert to establish policy solutions that can be used by all communities that are connected to the borderless cyber realm.

Chapter 3: Research Method

Introduction

The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for one international law for defining criminal hacking and the penalties associated with the act of criminal hacking. In this study, I sought to find meaningful relationships between the independent and dependent variables of the study (see Appendix A). Valuable insights were gained from the individuals surveyed about their attitudes toward the need for an international law in defining and penalizing criminal hacking, which could potentially be used to promote further research in the arena of international cooperation efforts toward implementing consistent universal policies and laws addressing criminal hacking in the borderless realm of information and communication technologies.

This chapter consists of the research design and rationale, methodology, data analysis plan, threats to validity, ethical procedures, and a summary of the chapter. The research design addressed the research scientifically, using descriptive and inferential research. The logic behind the methodology in participant selection included the knowledge of those involved in the entities chosen as well as the expertise of individual stakeholders relevant in the discipline of the study.

The components in the published instrumentation, provided through the Qualtrics statistical platform Stats iQ, addressed reliability and validity, while providing reliability evidence of internal consistency and testing and retesting, as well as validity evidence

through predictive and construct validity. Instrumentation sufficiency was established through the Qualtrics survey platform to help ensure each respondent had the ability to appropriately provide answers for the research questions of the study. Survey rating scales, including Likert and semantic differential scales, were used to address the study from a deductive reasoning approach. The data analysis plan encompassed the use of the Qualtrics statistical software for the survey and the analysis of the data. Ethical procedures were explained and approached using best standard practices put forth by the official institutional Internal Review Board (IRB), which included a consent form.

The setting involved a structured survey for quantitative data collection accessed through the reputable Qualtrics platform, which played a fundamental part in the structure of the research design for the study. Individual stakeholders in the public and private sectors, with some affiliation to cybersecurity through various organizations (see Appendix A), and their networking and social groups were provided survey questions through an anonymous link. These individual respondents represented a unique knowledge base in the cybersecurity realm, which encompassed various perspectives in relation to the study questions.

The survey (see Appendix B) was sent to security organizations and LinkedIn networks in cybersecurity, where the memberships and networks were made up of a vast array of individuals from public and private sectors, including various representatives from critical infrastructure sectors. These multidisciplinary memberships provided professional insights to the study with their expertise and knowledge for addressing the virtual context of the study in relation to the criminal acts of technological intrusions and

compromise, with an understanding that these acts can affect any given critical infrastructure or society.

The quantitative study examined individual attitudes toward an international law governing the cyber realm in relation to defining criminal hacking and the penalties associated with the act, and if there is a difference in the attitudes of individual respondents among public and private sectors. The independent variables of the study included age group, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education, which related to the hypotheses by providing, through correlation, what the relationship is between the dependent variables, of attitudes toward the need for international laws for defining criminal hacking and penalties, and the individuals associated with the public and private sectors, for the question of the study (see Appendix A).

Research Design and Rationale

Creswell (2016) advised detailing the core principles that should be included in the research design, including concerted efforts toward development, analysis of the problem, proactive planning of the research process through documentation, and suitable measures taken for implementing and evaluating the generalized conclusions through critical reasoning. This study provided a framework that incorporated best standard practices throughout the research process. Kanji (2006) explained that tests are not to be designed to gain an approval or disapproval of hypotheses but to show the hypotheses being tested are "untenable as it leads to an unsatisfactorily small probability" (p. 2). Osborne (2008, 2017) illustrated how best practices are crucial in research studies, which

helps provide informative and trustworthy results, provided the communication method is effective when demonstrating the results.

Mills (1992) illustrated the importance of understanding that science seeks the truth through an objective means, while questions of value are intended to be a part of the policy process, including problems associated with technological progress. Policy issues require concerted efforts between scientists and policy makers to define and address fundamental technical and policy elements, including the scientific community putting facts in order to assess problems and potential solutions; policy makers have the task of proposing effective legislation after considering all the varying values put forth (Mills, 1992). In the policy realm, decision makers have obligations to future generations in making the best decisions with relevant available information involving the expertise of various entities in the scientific community (Mills, 1992).

Due to the evolving nature of the threat landscape in the cyber world, issues are addressed in relation to the need for concerted unified global efforts in collectively coordinating universally consistent policies for the penalties of criminal hacking. The central concept of the study revolved around exploring the attitudes of individuals among the public and private sectors on the need to have an international law for defining criminal hacking, the need to have an international law for the punishments of criminal hacking, and to what extent the acts of criminal hacking should be penalized. Morse, Niehaus, Wolfe, and Wilkins (2006) clarified how a theoretical drive should be clearly defined in the study, which helps to ensure the direction of the research study is on track within the specific design.

Role theory was used as the theoretical drive to show how roles play a critical part in addressing the problems of criminal hacking. The rationale for the design of the study was chosen to gain perceptions and insights from the individual participant data for evaluating the need for an international law for defining criminal hacking and the punishments for the crimes, as well as fulfilling a gap in the literature in addressing international unified policy standards in the technological realm.

Structured closed-end question surveys were made available via e-mail invitation to various participants with ties to the cybersecurity realm to the memberships of several security organizations on behalf of the researcher, their networking groups, and LinkedIn networking groups with a cybersecurity professional presence served as the research sampling units. There was not a relationship of power over any of the proposed subjects for the study. The use of anonymous data collection, through a virtual survey, helped in obtaining responses that were accurate from the individual respondents. Any biases were managed by conducting the study in an objective manner, helping to ensure the true results of the nonexperimental research study were provided.

Study Variables

The following provides the independent variables (IVs), dependent variables (DVs), and groups for the study (See Appendix A).

DVs: The dependent variables for the study are:

- DV1: Attitudes toward the need for one international law for defining criminal hacking.

- DV2: Attitudes toward the need for the penalties of criminal hacking to be addressed under one international law?
- DV3: Attitudes toward the extent that criminal hacking should be penalized, given it would be implemented globally?

The independent variables for the study are:

- IV1 – Age group (ratio scale)
- IV2 – Ethnicity (nominal)
- IV3 – Gender (dichotomous)
- IV4 – Infrastructure sector affiliation (nominal)
- IV5 – Technical hacking ability (dichotomous)
- IV6 – Education (nominal)

The groups for the study are:

Groups – Employment sector (nominal)

- Public sector
- Private sector

Methodology

Population

The population for the study targeted multidisciplinary professionals from the public and private sectors who worked directly, indirectly, or had some knowledge in the security, cybersecurity, and legislative realms, as well as their networking groups and LinkedIn networks. Additionally, the Walden Research Participant Pool was approved and provided for an additional six respondents. The back-up sampling strategy was to

gain a sample population through the Qualtrics statistical platform, which supplies survey respondents for a charge, this option was not used in that there was an adequate number of respondents, gained through the initial sampling strategy. The initial sampling frame was chosen because the population is necessary for the scope of the study in gaining a representation of the knowledge base that made up those that can influence policy initiatives.

Sampling and Procedures

For this quantitative study, the sample size was determined prior to the dissemination of this survey. To determine the sample size the target population was determined, those that have some affiliation with the cybersecurity community. The population size can be hard to estimate in many cases and is unknown for the parameters of this study, therefore a standard equation was used to statistically determine the sample size.

The confidence level for the study was set at 95%, which is a good and recommended standard for scholarly studies, according to many statistical experts. 95% provides a Z Score that equals 1.96, for the numerical portion of the statistical equation for calculating the sample size, according to Qualtrics (Qualtrics, Determining Sample Size, par. 5, retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/). The standard of deviation, or the variance expected in the survey responses, was set at the standard of .5, given the adequate sample size. The margin of error, also known as the confidence interval, was set at +/- 5%. The following standard equation involving the z-score, standard of deviation,

and the confidence interval was used to determine the sample size for an unknown population size*(Qualtrics, Determining Sample Size, para. 4, retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/).

Necessary Sample Size = (Z-score)² * StdDev*(1-StdDev) / (margin of error)²

Using the above standard equation, with the parameters set for the study shown above, the following provides the statistical equation from the sample size formula according to the Qualtrics sample size calculation (Qualtrics, Determining Sample Size, para 6, retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/).

((1.96)² x .5(.5)) / (.05)²

(3.8416 x .25) / .0025

.9604 / .0025

384.16

385

It is sometimes necessary for researchers to adjust the parameters a bit for sample sizes that are too large, which increases the chances for errors from the sampling, which can be done by increasing your margin of error or decreasing your confidence level (Qualtrics, Determining Sample Size, retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/).

Similarly, Raosoft provided a sample size calculator that allows researchers to input the percentages of the margin of error (showing 5% as a common choice), confidence level (showing 90%, 95%, or 99% as choices), population size (using 20,000

for unknown population sizes), and response distribution, or standard of deviation at .5 (Raosoft Sample Size Calculator, retrieved from http://www.raosoft.com/samplesize.html). Using 5% as a margin of error to accept, 95% as the confidence level, 20,000 for the unknown population size, and 50% as the standard of deviation, the recommended sample size is 377 (Raosoft Sample Size Calculator, retrieved from http://www.raosoft.com/samplesize.html).

The quantitative survey was sent out to national, international, and statewide organizations that hold membership populations in the security realm as a sample population through the executive leadership of a number of non-profit organizations. Additional opportunities for the networking groups of these groups to be surveyed through referral sampling, was used as an additional sample for the sample population. An email was sent to these organizations and LinkedIn network groups inviting individual participation in the survey.

Procedures for Recruitment, Participation, and Data Collection

The procedures for recruitment, participation, and data collection included reaching out to executive board members of the various security organizations to gain approval to sample their membership population, which included public and private sectors individuals involved in various cybersecurity organizations. An email was sent to the members of these organizations by the leadership of the organization on behalf of the researcher, and LinkedIn network groups inviting individual participation in the survey.

Surveys were distributed and gained through a reputable survey platform, Qualtrics single user license, for the study. This survey platform allowed for a number of

distributions, if needed, as a back-up for a sample population for the study. The manual distribution, through the platform, provided a generic survey link and collected all responses anonymously. To help ensure respondents did not use the survey link multiple times, the option tab was selected, which prevented ballot box stuffing.

Instrumentation and Operationalization of Constructs

The quantitative instrumentation consisted of a structured survey with closed ended questions using survey Likert rating scales. The survey (see Appendix B) consisted of a researcher-developed questionnaire consisting of Likert and semantic differential rating scales administered through Qualtrics, a published reputable survey software platform. Using Qualtrics single user student license and Stats iQ (Qualtrics, Provo, UT, 2019 -2020) assisted in establishing consistency measures internally through the correlation of the data sets, including measures that addressed similarities within the questions being measured.

Operationalization for Variables

The independent variables (IVs), dependent variables (DVs), and groups for the study were operationalized and measured in a number of ways to show the correlations and relationship between variables. Independent Variables were nominally and dichotomously measured, as well as through ratio scale measurement. The independent variables, including the groups of the study, and the dependent variables from the survey results were coded for statistical analyses for determining the outcomes for the questions of the study.

Data Analysis Plan

Qualtrics stats IQ statistical software was used for the analysis for the research study. Validating the data through an auditing, repetitious process to ensure accuracy of the data input, which included the utilization of the Qualtrics platform for dataset examination. Kanji (2006) explained tests are not to be designed to gain an approval or disapproval of hypotheses, but to show the hypotheses being tested is "untenable as it leads to an unsatisfactorily small probability (Kanji, 2006, p. 2)." Expert mentoring through Walden University, in the quantitative process, was established and served as an audit element in helping to ensure reliability and validity throughout the quantitative process. The following provides the research questions and hypotheses for the study.

RQ1: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector entities?

$H_0$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector individuals?

$H_1$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector individuals?

RQ2: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_0$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_1$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

RQ3: Is there a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_0$3: There is no difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_1$3: There is a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

The appropriate calculated alpha, power, and effect size was determined, as well a calculated minimum sample size, prior to proceeding with running the statistical tests. The nominal, dichotomous and ratio scale survey outcomes were coded using the most current Qualtrics Stats iQ software database. The coded survey results were statistically tested. Datasets were formulated from the coded independent, dependent, and groups input for analysis in determining if the null hypotheses would be accepted or if the null hypotheses would be rejected and the alternative hypotheses accepted, for each question of the study in Chapter 4.

Chi-squared statistical analysis was run providing the statistical data needed for the results of the study. Descriptive statistical analysis was conducted through data observation and compared and contrasted through inferential statistical analysis. The quantitative process provided for deductive data analysis, as well as provided a platform for objectivity within the elemental processes of the study. Concerted efforts were taken to help ensure there were no Type I or Type II errors in the testing procedures. Type I errors involve rejecting a true hypothesis due to testing procedures and Type II errors involve rejecting a false null hypothesis due to testing procedures. It has been stated by a number of experts, in relation to a courtroom illustration, that making a Type I error is

like an innocent defendant being convicted and making a Type II error is like letting a criminal go free, by gaining an acquittal.

Threats to Validity

External validity was addressed through generalizability, where the threats may include not examining the results of a study against the results of similar studies to show how the findings apply to the answers of the research questions.

Ihantola and Kihn (2011) illustrated how an appropriate research design is critical for the context of the study for providing a framework that mitigates the threats to validity. Threats to internal validity can take place any time during the study, which could include a lack of knowledge in relation to the study, where the logic presented is contradictory to most of the research, or toward the end of the study when interpreting and analyzing the data (Ihantola & Kihn, 2011). Ihantola and Kihn (2011) displayed, through the studies of (Campbell & Stanely 163 in, Tashakkori & Teddlie, 1998, p.87) that issues with instrumentation can pose a threat to internal validity in the data collection phase. Through the study of (Onwuegbuzie, 2003) Ihantola and Kihn (2011) showed how bias can influence a study using technological tools and the way in which the researcher chooses to interpret the findings according to their preferred techniques.

Steps were taken to help provide a holistic representative for capturing of the data, in efforts to ensure the credibility of the findings, including procedural reliability, with auditing expertise in the analysis of the statistical processes. (Inhantola & Kihn, 2011; Öhlén, 2011). Statistical expertise was sought throughout the quantitative portion of the

study to help ensure validity, credibility for the internal validity and transferability for the external validity.

Questions that should be answered in relation to the assumptions of the quantitative paradigm include looking at the study through lenses ontologically, epistemologically, axiological, rhetorically, and methodologically (Creswell, 2014). Creswell (2014) stated addressing the question of reality should be objectively examined, the assumption that the researcher will be independent from the study, role assumption should be unbiased and free of values, the language of the research should be formal and quantitatively impersonal, and the methodological assumption of the study should ensure the research encompasses a deductive process through generalizations, validity, and reliability.

Ethical Procedures

Agreement documents for participants were formulated to comply with Internal Review Board (IRB) standards for the treatment of participants in the study and were included in the IRB application. Approvals and permissions were granted by the IRB before the start of the proposed study. Ethical elements were addressed throughout every stage of the study according to the official institutional IRB best standard practices and protocols.

A formal email was sent electronically, through the associations and LinkedIn networks on behalf of the researcher, describing the purpose of the study and why it is relevant today with an anonymous survey link inviting individuals to be a voluntary participant in the study. The survey link took all individual volunteers to the survey (see

Appendix B). The survey was completely anonymous, including not capturing the IP addresses of those responding to the survey. This was made possible by selecting this option through the Qualtrics platform.

Privacy risks were minimal in that the survey respondents were completely anonymous. By sending a survey link to various security organizations and asking for the leadership of each organization to send an invitation on the behalf of the researcher to participate in the study through a survey link, added to the anonymous nature of the study, including the option of not capturing IP addresses, through the Qualtrics platform. All survey responses were anonymous and voluntary, including the exclusion of IP address identifiers, and presented minimal risks. The use of anonymity measures helped ensure there were no potential conflicts of interest. Measures were taken to mask the names of the various organizations that participated in the study according to the Walden University IRB best practices.

Summary of Design and Methodology

The methodology chosen for this research study offered a framework for gaining some insights from a multidisciplinary sample of individuals from the private and public sectors that were familiar with cybersecurity related issues. This study generated insights and knowledge for addressing the problem of criminal hacking globally and the potential to help in future studies to show how policies and laws should be crafted in the future. Through capturing the insights of individuals among the public and private sectors, and their networking connections, on their attitudes for the need of an international law for defining criminal hacking, the penalties associated with the act, and to what extent

criminal hacking should be punished a foundation has been established that can be built upon. The insights gained helped distinguish if there is a need for one international law addressing criminal hacking or if increased coordinative efforts toward addressing criminal hacking from a singular nation's multinational coordinative approach is needed.

Using the quantitative research design provided the generalizable scientific *truth* of what perceptions are held among various disciplines for the protection of the cyber realm, including those immersed in cybersecurity professions, law enforcement, academia, the legislative realm, to name a few. Special attention was provided to the threats to validity and how to mitigate those threats through the structured quantitative research design. Concerted efforts were put forth to help ensure all the ethical procedures involved for the participants in the study were covered using best standard practices of the official institutional IRB. The deductive logic derived from the research questions garnered insight to be synthesized for helping to propel future decision-making processes nationally and internationally for the cybersecurity policy domain in addressing criminal hacking. In chapter 4 the quantitative results are presented.

Chapter 4: Results

Introduction

The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for one international law defining criminal hacking and the penalties associated with the acts of criminal hacking and to what extent the crime should be penalized. The research questions were designed to gain insight from public and private sector individuals on their attitudes toward the need for an international law defining criminal hacking, the penalties associated with the acts of criminal hacking, and to what extent criminal hacking should be punished. The independent variables of the study included age group, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education; they were statistically measured with the dependent variables of the study and the groups of public and private sector entities, showing correlations for the questions of the study.

The following provides the central research question and the three questions for the study: Is there a need for the definition of criminal hacking and the penalties associated with the act to be addressed under one international law?

RQ1: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector entities?

$H_0$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for one

international law for defining criminal hacking between public and private sector individuals?

$H_1$1: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector individuals?

RQ2: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_0$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do not predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

$H_1$2: Age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education do predict the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law between public and private sector individuals?

RQ3: Is there a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_0$3: There is no difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

$H_1$3: There is a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

Chapter 4 consists of the data collection details, descriptive statistics for the survey questions, and the results of the study. The data collection details include the time frame for data collection and the rates for recruitment and response, descriptive and demographic characteristics of the sample, a description of how the sample related to the population of interest, and challenges in the recruitment process. The results of the study provide descriptive statistics that characterized the sample, an evaluation of statistical assumptions, and statistical analyses findings with tables and figures illustrating the results.

Data Collection

Walden University approved the study on July 12, 2019. The approval number for this study is 07-16-19-0324940 and it expires on July 15, 2020. The survey data were collected over a 5-month period through responses received from the memberships of a

number of security organizations through an invitation sent on my behalf, LinkedIn responses to the posted study on LinkedIn, and six responses through the Walden University participant pool. The response rates were minimally steady throughout the process, with some peaks in the response rates during the period likely because some respondents reposted the survey request on their LinkedIn platforms. I assume the majority of the responses were from security organizations because response rates peaked when surveys were sent to those organizations' memberships.

The sample included various demographic characteristics according to those options provided in the survey questions, which included men and women; age group representations from 18 years and above; educational backgrounds; and originating ethnicities, which included Asian, African, American, Australian, Canadian, European Union, Hispanic or Latino, India National, Middle Eastern, Russian, and the option of other. Additionally, the sample included employment in public or private sector; critical infrastructure most affiliated with, which included chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, education sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors materials and waste sector, transportation systems sector, water and wastewater systems sector, and the option of not being affiliated with any of the infrastructures provided above. The options of technical hacking ability or no technical hacking ability were also captured.

Purposive total population nonprobability sampling was used for the study. The sample studied represented a population of those affiliated with cybersecurity or security in general to varying degrees. The population of interest represented only a portion of the larger population, providing for a representative sample, given the scope of the study, to gain the attitudes of individuals in the public and private sectors on international laws for criminal hacking. The sample comprised of individual members of a number of security organizations, LinkedIn professional networks, and a small sample of six respondents from the Walden University participant pool. Sibona and Walczak (2012) showed how using social networking sites for sample population, through nonprobability recruitment, can help in exploring newer ideas pertaining to technologies and different cultures. It is unknown if external validity or generalizability can be applied to all groups outside the realm of cybersecurity or security in general. Hard to reach populations, such as the criminal hacking realm, may have provided attitudes different from those represented in this study.

The survey was administered according to the method planned for the sample population, which included requests from security-related organizations to send out a request to their membership on my behalf and LinkedIn networks comprising of those familiar with security. Several organizations accepted the invitation to disseminate the survey, and a few declined due to policies in place to only disseminate the organization's proprietary surveys to members. Although the length of time to gain a sizable number of respondents was a challenge, the survey was open for 5 months and captured 228 responses.

Challenges in gaining survey respondents could be due to the reasons some security professionals tend to not participate in surveys or questionnaires. According to a study on privacy, Heikkila (2009) illustrated 30 responses to her open ended follow up question on why so few respond to security related questionnaires. The following is a list of several of the responses (Heikkila, 2009, p. 91, Table 5):

- "Because we don't know who will have access to identifying information from the survey and we don't want to advertise our vulnerabilities."
- "People get asked to fill out surveys every day."
- "Not enough time to respond to surveys."
- "Fear that the information will be used against them. Embarrassment. Ignorance on the subject. Many do not understand security and assume someone is taking care of it."

Results

The descriptive statistics that characterized the sample for the study enabled for a clear picture to be gained from all the initial data inputs. The following tables provide the demographics of the respondents in relation to employment sector affiliation (Table 1) and for each of the ten individual survey questions answered (Tables 2-11).

The following provides an example for reading the demographics table (Table 1). Of the nongovernmental organization group, 0.0% are 18 to 29 years of age, 18.8% are 30 to 39 years of age, 31.3% are 40 to 49 years of age, 31.3% are 50 to 50 years of age, and 18.8% are 60 years of age and above, which totals 100% for the number of respondents that chose the nongovernmental organization as their employment sector.

Table 1

Frequency Counts on the Demographics of Respondents in Relation to the Groups of the Study: Employment Sector Affiliation, N = 226

Demographics	Nongovernmental organization	Private sector	Public sector	Retired	Unable to work
Age group N = 226					
18–29 years	0.0	5.2	0.0	0.0	0.0
30–39 years	18.8	16.4	22.1	0.0	33.3
40–49 years	31.3	29.1	36.8	0.0	33.3
50–59 years	31.3	35.8	27.9	40.0	33.3
60 years and above	18.8	13.4	13.2	60.0	0.0
Ethnicity N = 226					
African	12.5	2.2	4.4	0.0	0.0
American	43.8	64.2	67.6	40.0	66.7
Asian	6.3	4.5	0.0	0.0	0.0
Canadian	0.0	1.5	2.9	0.0	0.0
EU	6.3	19.4	16.2	40.0	0.0
Hispanic	12.5	0.7	1.5	0.0	0.0
India National	0.0	0.7	1.5	0.0	0.0
Middle Eastern	12.5	0.7	2.9	0.0	0.0
Other	6.3	6.0	2.9	20.0	33.3
Gender N = 225					
Female	25.0	24.6	23.9	20.0	100.0
Male	75.0	75.4	76.1	80.0	0.0
Infrastructure affiliation N = 225					
Chemical	0.0	1.5	0.0	0.0	0.0
Commercial facilities	0.0	3.7	0.0	20.0	0.0
Communications	0.0	0.7	2.9	0.0	0.0
Critical manufacturing	0.0	5.2	0.0	0.0	0.0
Defense industrial base	0.0	2.2	1.5	0.0	0.0
Education	31.3	7.5	20.6	20.0	0.0
Emergency services	0.0	0.7	4.4	0.0	0.0
Energy	0.0	3.7	1.5	0.0	0.0
Financial services	0.0	11.2	2.9	0.0	0.0
Food and agriculture	0.0	3.0	0.0	0.0	0.0
Government facilities	6.3	0.0	14.7	0.0	0.0
Healthcare and public health	25.0	9.0	14.7	20.0	0.0
Information and technologies	18.8	39.6	29.4	20.0	0.0
Transportation	0.0	2.2	0.0	0.0	0.0
Other	18.8	9.7	7.4	20.0	0.0
Technical hacking ability N = 224					
Yes	50.0	47.8	47.8	25.0	0.0
No	50.0	52.2	52.2	75.0	100.0
Education N = 225					
Diploma or equivalent	6.3	4.5	1.5	0.0	0.0
Trade/technical training or college degree	37.5	53.4	52.9	60.0	66.7
Master's degree or higher	56.3	42.1	45.6	40.0	33.3

Note. N = Total respondents for each demographic category.

For *Survey Q1* (see Appendix B) there were 226 respondents who chose to answer the question out of 228 total survey responses, and two who chose not to answer the question on age group. Of the 226 responses, 7 (3.1 %) responded in the 18-29 age bracket, 41 (18.1%) responded in the 30-39 age bracket, 70 (31%) responded in the 40 – 49 age bracket, 75 (33.2%) responded in the 50-59 age bracket, and 33 (14.6%) responded in the 60 years and above age bracket. The table shows the majority of the respondents fall within the 40 to 59 age bracket (Table 2).

Table 2

Frequency Counts for Independent Ratio Scale Variable: Age Group

Age group	n	%	% of Data: confidence interval
18 to 29 years	7	3.1	1.9 to 4.9
30 to 39 years	41	18.1	15.1 to 21.7
40 to 49 years	70	31.0	27.2 to 35.0
50 to 59 years	75	33.2	29.3 to 37.3
60 years and above	33	14.6	11.8 to 17.9

Note. $N = 226$.

For *Survey Q2* (see Appendix B) there were 226 respondents who chose to answer the question out of 228 total survey responses, and two that chose not to answer the question on ethnicity. Of the 226 responses, 8 (3.5 %) responded to African descent, 143 (63.3%) responded to American descent, 7 (3.1%) responded to Asian descent, 4 (1.8%) responded to Canadian descent, 40 (17.7%) responded to European Union descent, 4 (1.8%) responded to Hispanic or Latino descent, 2 (0.88%) responded to India National

descent, 5 (2.2%) responded to Middle Eastern descent, and 13 (5.8%) responded to other. The table shows the majority of respondents are from American descent (Table 3).

Table 3

Frequency Counts for Independent Nominal Variable: Ethnicity

Ethnicity	n	%	% of Data: confidence interval
African	8	3.5	2.3 to 5.5
American	143	63.3	59.1 to 67.3
Asian	7	3.1	1.9 to 4.9
Canadian	4	1.8	0.9 to 3.3
EU	40	17.7	14.7 to 21.2
Hispanic	4	1.8	0.9 to 3.3
India National	2	0.88	0.4 to 2.1
Middle Eastern	5	2.2	1.3 to 3.9
Other	13	5.8	4.1 to 8.1

Note. $N = 226$.

For *Survey Q3* (see Appendix B) there were 225 respondents who chose to answer the question out of 228 total survey responses, and three that chose not to answer the question on gender. Of the 225 responses, 168 (74.7 %) responded to being male and 57 (25.3%) responded to being female. The table shows nearly 3/4 of the survey respondents were male (Table 4).

Table 4

Frequency Counts for Independent Dichotomous Variable: Gender

Gender	n	%	% of Data: Confidence Interval
Male	168	74.7	70.8 to 78.2
Female	57	25.3	21.8 to 29.2

Note. $N = 225$

For *Survey Q4* (see Appendix B) there were 225 respondents who chose to answer the question out of 228 total survey responses, and three that chose not to answer the question on infrastructure affiliation. Of the 225 responses, 2 (0.88 %) responded being affiliated with the chemical sector, 6 (2.7%) responded to being affiliated with the commercial facilities sector, 3 (1.3%) responded to being affiliated with the communications sector, 7 (3.1%) responded to being affiliated with the critical manufacturing sector, 4 (1.8%) responded to being affiliated with defense industrial base sector, 30 (13.3%) responded to being affiliated with the education sector, 4 (1.8%) responded to being affiliated with the emergency services sector, 6 (2.7%) responded to being affiliated with the energy sector, 17 (7.5%) responded to being affiliated with the financial services sector, 4 (1.8%) responded to being affiliated with the food and agriculture sector, 11 (4.9%) responded to being affiliated with the government facilities sector, 27 (11.9%) responded to being affiliated with the healthcare and public health sector, 77 (34.1%) responded to being affiliated with the information technology sector, 3 (1.3%) responded to being a part of the transportation sector, and 25 (11.1%) responded to other, or not being affiliated with any of the infrastructure sectors provided (Table 5).

Table 5

Frequency Counts for Independent Nominal Variable: Infrastructure Sector Affiliation

Infrastructure sector affiliation	n	%	% of Data: confidence interval
Chemical	2	0.88	0.4 to 2.1
Commercial facilities	6	2.7	1.6 to 4.4
Communications	3	1.3	0.6 to 2.7
Critical manufacturing	7	3.1	1.9 to4.9
Defense industrial base	4	1.8	0.9 to 3.3

Education	30	13.3	10.6 to 16.4
Emergency services	4	1.8	0.9 to 3.3
Energy	6	2.7	1.6 to 4.4
Financial services	17	7.5	5.6 to 10.1
Food and agriculture	4	1.8	0.9 to 3.3
Government facilities	11	4.9	3.3 to 7.0
Healthcare and public health	27	11.9	9.5 to 15.0
Information and technologies	77	34.1	30.2 to 38.2
Transportation	3	1.3	0.6 to 2.7
Other	25	11.1	8.7 to 14.0

Note. N = 225

For *Survey Q5* (see Appendix B) there were 224 respondents who chose to answer the question out of 228 total survey responses, and four chose not to answer the question on technical hacking ability. Of the 224 responses, 105 (46.9 %) responded to having technical hacking ability, and 119 (53.1%) responded to not having technical hacking skills. The table shows nearly an even distribution of technical hacking ability and no technical hacking skills among the survey respondents (Table 6).

Table 6

Frequency Counts for Independent Dichotomous Variable: Technical Hacking Ability

Technical hacking ability	n	%	% of Data: confidence interval
Technical hacking ability	105	46.9	42.6 to 51.2
No technical hacking skills	119	53.1	48.8 to 57.4

Note. N = 224.

For *Survey Q6* (see Appendix B) there were 225 respondents that chose to answer the question out of 228 total survey responses, and two who chose not to answer the question on education. Of the 225 responses, 8 (3.6 %) responded to having a high school graduate degree or equivalent, 99 (44.0%) responded to having a Master's degree or higher, and 118 (52.4%) responded to having trade or technical training or a college degree. The table shows 96.4 % of the respondents achieved education outside of the high school graduate level (Table 7).

Table 7

Frequency Counts for Independent Nominal Variable: Education

Education	n	%	% of Data: confidence interval
High school graduate or equivalent	8	3.6	2.3 to 5.5
Master's degree or higher	99	44.0	39.8 to 48.3
Trade/technical training or a college degree	118	52.4	48.2 to 56.7

Note. $N = 225$.

For *Survey Q7* (see Appendix B), 226 respondents chose to answer the question out of 228 total survey responses, and two chose not to answer the question on employment sector. Of the 226 responses, 134 (59.3 %) responded to being a part of the private sector, 68 (30.1%) responded to being a part of the public sector, 16 (7.1%) responded to having being a part of a non-governmental organization, 5 (2.2%)

responded to being retired, and 3 (1.3%) responded to being unable to work. Nearly 2/3 of the respondents are from the private sector (Table 8).

Table 8

Frequency Counts for Groups Nominal Variable: Employment Sector

Employment sector	n	%	% of Data: confidence interval
Private sector	134	59.3	55.1 to 63.4
Public sector	68	30.1	26.3 to 34.1
NGO	16	7.1	5.2 to 9.6
Retired	5	2.2	1.3 to 3.9
Unable to work	3	1.3	0.6 to 2.7

Note. $N = 226$.

For *Survey Q8* (see Appendix B) there were 224 respondents who chose to answer the question, out of 228 total survey responses, and four chose not to answer the question.

Research Question 1: On a scale from 1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking (See Appendix B, *Survey Q8*)?

Of the 224 responses, 104 (46.4 %) responded strongly agree, 80 (35.7%) responded somewhat agree, 14 (6.3%) responded to neither agree nor disagree, 14 (6.3%) responded to somewhat disagree, 12 (5.4%) responded to strongly disagree (Table 9).

Table 9

Frequency Counts for Dependent Variable: Research Question 1, Likert Scale

RQ1	n	%	% of Data: confidence interval
Strongly agree	104	46.4	42.2 to 50.7

Somewhat agree	80	35.7	31.7 to 39.9
Neither agree nor disagree	14	6.3	4.5 to 8.7
Somewhat disagree	14	6.3	4.5 to 8.7
Strongly disagree	12	5.4	3.7 to 7.6

Note. $N = 224$.

Numerical coding of RQ1 in Stats iQ allowed for the following descriptive statistics for the dependent variable Likert scale evaluation of *Survey Q8* (Table 10).

Table 10

Numerically Coded Dependent Variable: Survey Question 8 - Likert Scale

Sample size	Medium	Average	Confidence interval of average	Standard deviation	Min	Max	Sum
224	2.0	1.88	1.74 – 2.03	1.12	1.0	5.0	422

For *Survey Q9* (see Appendix B) there were 226 respondents who chose to answer the question, out of 228 total survey responses, and two chose not to answer the question.

Research Question 2: On a scale from 1 to 5 please indicate how you would rate your attitude toward the need for the penalties of criminal hacking to be addressed under one international law (see Appendix B, *Survey Q9*)?

Of the 226 responses, 102 (45.1 %) responded strongly agree, 80 (35.4%) responded somewhat agree, 14 (6.2%) responded to neither agree nor disagree, 15 (6.6%) responded to somewhat disagree, 15 (6.6%) responded to strongly disagree (Table 11).

Table 11

Frequency Counts for Dependent Variable: Research Question 2 - Likert Scale

RQ2	n	%	% of Data: confidence interval
Strongly agree	102	45.1	40.9 to 49.4
Somewhat agree	80	35.4	31.4 to 39.6
Neither agree nor disagree	14	6.2	4.4 to 8.6
Somewhat disagree	15	6.6	4.8 to 9.1
Strongly disagree	15	6.6	4.8 to 9.1

Note. $N = 226$.

Numerical coding of RQ1 in Stats iQ allowed for the following descriptive statistics for the dependent variable Likert scale evaluation of *Survey Q9* (Table 12).

Table 12

Numerically Coded Dependent Variable: Survey Question 9 - Likert Scale

Sample size	Medium	Average	Confidence interval of average	Standard deviation	Min	Max	Sum
226	2.0	1.94	1.79 – 2.10	1.17	1.0	5.0	439

For *Survey Q10* (see Appendix B) there were 225 respondents who chose to answer the question out of 228 total survey responses, and three chose not to answer the question.

Research Question 3: On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it would

be implemented globally? Use the example of the United States Computer Fraud and Abuse Act (CFAA) penalties chart (see Appendix B, *Survey Q10*).

Of the 225 responses, 4 (1.8 %) responded no penalties, 7 (3.1%) responded minimal to less than moderate penalties, 61 (27.1%) responded to moderate penalties, 98 (43.6%) responded to more than moderate penalties, and 55 (24.4%) responded to the harshest of penalties (Table 13).

Table 13

Frequency Counts for Dependent Variable: Research Question 3 - Likert Scale

RQ3	n	%	% of Data: confidence interval
No Penalties	4	1.8	.9 to 3.3
Minimal to Less Than Moderate Penalties	7	3.1	1.9 to 5.0
Moderate Penalties	61	27.1	23.5 to 31.1
More Than Moderate Penalties	98	43.6	39.4 to 47
Harshest of Penalties	55	24.4	21.0 to 28.3

Note. $N = 225$.

Numerical coding of RQ1 in Stats iQ allowed for the following descriptive statistics for the dependent variables of survey questions 10 through 12 Likert scale evaluations (Tables 14-16).

Table 14

Numerically Coded Dependent Variable: Survey Question 8 - Likert Scale

Sample Size	Medium	Average	Confidence Interval of Average	Standard Deviation	Min	Max	Sum
224	2.0	1.88	1.74 – 2.03	1.12	1.0	5.0	422

Note. Code 1 = strongly agree. Code 2 = somewhat agree. Code 3 = neither agree nor disagree. Code 4 = disagree. Code 5 = strongly disagree.

Table 15

Numerically Coded Dependent Variable: Survey Question 9 - Likert Scale

Sample Size	Medium	Average	Confidence interval of average	Standard deviation	Min	Max	Sum
226	2.0	1.94	1.79 – 2.10	1.17	1.0	5.0	439

Note. Code 1 = strongly agree. Code 2 = somewhat agree. Code 3 = neither agree nor disagree. Code 4 = disagree. Code 5 = strongly disagree.

Table 16

Numerically Coded Dependent Variable: Survey Question 10 - Likert Scale

Sample Size	Medium	Average	Confidence Interval of Average	Standard Deviation	Min	Max	Sum
225	4.0	3.86	3.74 – 3.97	0.89	1.0	5.0	868

Note. Code 1 = no penalties. Code 2 = minimal to less than moderate penalties. Code 3 = moderate penalties. Code 4 = more than moderate penalties. Code 5 = harshest of penalties.

The statistical platform used for the study was Stats iQ, a part of the Qualtrics platform. There are four options in Stats iQ for data analysis, which include describe, relate, regression, and pivot table. The artificial intelligence (AI) of the Stats iQ platform automatically defaults to the test with the least assumptions, given there is an option (Qualtrics, Provo, UT). The Stats iQ platform uses one-way ANOVA (Welch's F test) to

show relationships between two variables and Games-Howell tests to show if there are higher values in pairs of groups or others (Qualtrics, Provo, UT). In ranked correlation Stats iQ uses Spearman's Rho when assumptions are violated by implementing rank-transformation (Qualtrics, Provo, UT). "Rank transformation is a well-established method for protecting against assumption violation (a "nonparametric" method), and the rank transformation from Pearson to Spearman is the most common" (Conover and Iman, 1981, as cited by Qualtrics, Provo, UT). Pearson's r is used for Likert scale analysis, in that they are measured as they are continuous instead of ordinal, which is commonly done in the social science realm (Qualtrics, Provo, UT).

Chi-square statistical analysis was used on the respondent data to find correlations among the data points, which included the aforementioned statistical tests with the AI Stats iQ platform. The statistical assumption for analysis using chi-square is "there has to be at least five observations in each cell of the 2X2 table associated with the analysis (scalelive.com)." A Fisher's Exact Test is used when the aforementioned is not fulfilled (scalelive.com). The primary inference with Chi-square is 95% confidence level and unadjusted odds ratio (Qualtrics, Provo, UT).

Summary of *Survey Q8*: On a scale from 1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking?

The results of the chi-square analysis revealed a non-significant association relationship between *Survey Q7*: Employment Sector - Please specify the employment sector you are most closely aligned with, and RQ1, which is *Survey Q8*: On a scale from

1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking?

The analysis also showed no statistical significance with the independent variables of age group, ethnicity, gender, hacking ability, and education. Additionally, the relationship between *Survey Q7*: Employment Sector and *Survey Q4*: Infrastructure Sector showed there is a strong statistically significant relationship (Table 17). The following cells were statistically significant (Table 18):

- Of those that responded in the Private Sector group, 5.2% are in the Critical Manufacturing Sector group. The 95% Confidence interval is 2.6% to 10.4%.
- Of those that responded in the Public Sector group, 20.6% are in the Education Sector group. The 95% confidence interval is 12.7% to 31.6%.
- Of those that responded in the Non-Governmental Organization group, 31.3% are in the Education Sector group. The 95% Confidence interval is 14.2% to 55.6%.
- Of those that responded in the Private Sector group, 36.6% are in the Information Technology group. The 95% Confidence interval is 31.7 to 48.0%.

Table 17

Chi-square Test on Employment Sector (Survey Q7) and Infrastructure Affiliation (Survey Q4)

	Basic	Advanced
Statistical significance (P-Value)	Very clearly significant	0.000561
Effect size	Large	0.32753

(Cramér's V)

Note. Sample Size 226.

Table 18

The Relationship between Employment Sector and Infrastructure Sector Affiliation

Infrastructure sector affiliation	Nongovernmental organization	Private sector	Public sector	Retired
Chemical	0.0%	1.5%	0.0%	0.0%
Commercial facilities	0.0%	3.7%	0.0%	20.0%
Communications	0.0%	0.75%	2.9%	0.0%
Critical manufacturing	0.0%	5.2%	0.0%	0.0%
Defense industrial base	0.0%	2.2%	1.5%	0.0%
Education	31.3%	7.5%	20.6%	20.0%
Emergency services	0.0%	0.75%	4.4%	0.0%
Energy	0.0%	3.7%	1.5%	0.0%
Financial services	0.0%	11.2%	2.9%	0.0%
Food and agriculture	0.0%	3.0%	0.0%	0.0%
Government facilities	6.3%	0.0%	14.7%	0.0%
Healthcare and public health	25.0%	9.0%	14.7%	20.0%
Information and technologies	18.8%	39.6%	29.4%	20.0%
Transportation	0.0%	2.2%	0.0%	0.0%
Other	18.8%	9.7%	7.4%	20.0%

Using a 95% confidence level, the results of the chi-square analyses revealed no significant associations between the groups of the study (Public Sector, Private Sector, and Non-Governmental Organizations) and the independent and dependent variables of age group, ethnicity, gender, hacking ability, education, and *Survey Q8*: On a scale from 1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking? The chi-square statistical results: X^2 (16, N = 224) = 18, p = .32. There is no statistically significant association between the groups

of the employment sector and the dependent variable, RQ1 and *Survey Q8* of the study; therefore, I concluded the $H_0$1 cannot be rejected (Tables 19 & 20).

Table 19

Chi-square Test on Employment Sector (Survey Q7) and RQ1 (Survey Q8)

	Basic	Advanced
Statistical significance (P-Value)	Not significant	0.322249
Effect size (Cramér's V)	Small	0.32753

Note. Sample Size 224.

Table 20

Chi-squared Results

Chi square 18.0
Degrees of freedom 16

Summary of *Survey Q9*: On a scale from 1 to 5 please indicate how you would rate your attitude toward the need for the penalties of criminal hacking to be addressed under one international law?

Using a 95% confidence level, the data analysis showed no statistically significant relationship between *Survey Q7*: Employment Sector - Please specify the employment sector you are most closely aligned with, and *Survey Q9*: On a scale from 1 to 5 please indicate how you would rate your attitude toward the need for the penalties of criminal hacking to be addressed under one international law?

The analysis also showed no statistical significance among the groups of the study and the independent variables of age group, ethnicity, gender, infrastructure affiliation, hacking ability, education. The chi-square statistical results for the group of employment sector and RQ2: X^2 (16, N = 226) = 12.6, p = .70. There is no statistically significant association between the groups of the employment sector and dependent variable, RQ2 and *Survey Q9* of the study; therefore, I concluded the H02 cannot be rejected for RQ2. (Tables 21 & 22).

Table 21

Chi-square Test on Employment Sector (Survey Q7) and RQ2 (Survey Q9)

	Basic	Advanced
Statistical Significance (P-Value)	Not Significant	0.703178
Effect size (Cramér's V)	Small	0.117966

Note. Sample Size 226.

Table 22

Chi-squared Results

Chi square 12.6
Degrees of freedom 16

Summary of *Survey Q10*: On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it

would be implemented globally? See the United States Computer Fraud and Abuse Act (CFAA) penalties chart (see Appendix B)

Using a 95% confidence level, the data analysis showed no statistically significant relationship between Q7: Employment Sector - Please specify the employment sector you are most closely aligned with, and Q10: On a scale from 1 to 5 please indicate how you would rate your attitude toward the need for the penalties of criminal hacking to be addressed under one international law (Tables 23 & 24)?

The analysis also showed no statistical significance among the groups of the study and the independent variables of age group, ethnicity, gender, infrastructure affiliation, hacking ability, education. The chi-square statistical results for the group of employment sector and RQ3: X^2 (16, N = 225) = 21.9, p = .147. There is no statistically significant association between the groups of the employment sector and dependent variable, RQ3 and *Survey Q10* of the study; therefore, I concluded the H03 cannot be rejected for RQ3.

Table 23

Chi-square Test on Employment Sector (Survey Q7) and RQ3 (Survey Q10)

	Basic	Advanced
Statistical significance (P-Value)	Not significant	0.147
Effect Size (Cramér's V)	Small	0.156

Note. Sample Size 225.

Table 24

Chi-squared Results

Chi square 21.9
Degrees of freedom 16

Interestingly, the data analyses provided additional statistical correlation among the independent and dependent variables of the study showing varying degrees of significant relationships from the respondent's survey data. The following tables provided the results of the chi-square analyses using a 95% confidence level.

There is a statistically significant relationship between *Survey Q1*: Age Group and *Survey Q8*: On a scale from 1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking? The chi-square statistical results for age group and Q8: X^2 (16, N = 224) = 28.1, p = .0308

The chi-square statistical analyses and a pivot table showing the descriptive statistics are provided (Tables 25-27).

Table 25

Chi-square Test on Age Group (Survey Q1) and RQ1 (Survey Q8)

	Basic	Advanced
Statistical significance (P-Value)	Clearly significant	0.0308
Effect size (Cramér's V)	Medium	0.177

Note. Sample Size 224.

Table 26

Chi-squared Results

Chi square 28.1	
Degrees of freedom 16	

Table 27

Pivot Table for Age Group (Survey Q1) and RQ1 (Survey Q8)

Years of age	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
18 to 29	1.9%	3.8%	0.0%	7.1%	8.3%
30 to 39	10.6%	26.3%	50.0%	7.1%	8.3%
40 to 49	35.6%	28.8%	28.6%	14.3%	33.3%
50 to 59	33.7%	30.0%	7.1%	57.1%	41.7%
60 and up	18.3%	11.3%	14.3%	14.3%	8.3%
Total	0.100%	0.100%	0.100%	0.100%	0.100%

There is a strong statistically significant relationship between *Survey Q4*: Infrastructure Sector Affiliation and *Survey Q10*: On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it would be implemented globally? The chi-square statistical results for infrastructure affiliation and RQ3: X^2 (56, N = 225) = 84.2, p = .00882

The chi-square statistical analyses and a pivot table showing the descriptive statistics are provided (Tables 28-30).

Table 28

Chi-square Test on Infrastructure Affiliation (Survey Q4) and RQ3 (Survey Q10)

	Basic	Advanced
Statistical significance (P-Value)	Very clearly significant	0.00882
Effect size (Cramér's V)	Large	0.306

Note. Sample Size 225.

Table 29

Chi-squared Results

Chi square 84.2
Degrees of freedom 56

Table 30

Pivot Table for Infrastructure Affiliation (Survey Q4) and RQ3 (Survey Q10)

Infrastructure sector affiliation	Harshest of penalties	More than moderate penalties	Moderate penalties	Minimal to less than moderate	No penalties
Chemical	1.8%	1.0%	0.0%	0.0%	0.0%
Commercial facilities	3.6%	2.0%	1.6%	14.3%	0.0%
Communications	1.8%	2.0%	0.0%	0.0%	0.0%
Critical manufacturing	3.6%	1.0%	6.6%	0.0%	0.0%
Defense industrial base	1.8%	0.0%	3.3%	0.0%	25.0%
Education	7.3%	20.4%	4.9%	42.9%	0.0%
Emergency services	7.3%	0.0%	0.0%	0.0%	0.0%
Energy	3.6%	3.1%	1.6%	0.0%	0.0%

Financial services	10.9%	5.1%	6.6%	0.0%	50.0%
Food and agriculture	1.8%	2.0%	1.6%	0.0%	0.0%
Government facilities	1.8%	9.2%	1.6%	0.0%	0.0%
Healthcare and public health	10.9%	8.2%	21.3%	0.0%	0.0%
Information and technologies	29.1%	33.7%	39.3%	42.9%	25.0%
Transportation	0.0%	1.0%	3.3%	0.0%	0.0%
Other	14.5%	11.2%	8.2%	0.0%	0.0%
Total	100.0%	100%	100%	100%	100%

There is a statistically significant relationship between *Survey Q1*: Age Group and *Survey Q10*: On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it would be implemented globally? The chi-square statistical results for age group and RQ3: X^2 (16, N = 225) = 32.1, p = .00968

The chi-square statistical analysis and a pivot table showing the descriptive statistics are provided (Tables 31-33).

Table 31

Chi-square Test on Age Group (Survey Q1) and RQ3 (Survey Q10)

	Basic	Advanced
Statistical significance (P-Value)	Very clearly significant	0.00968
Effect size (Cramér's V)	Medium	0.189

Note. Sample Size 225.

Table 32

Chi-squared Results

Chi square 32.1	
Degrees of freedom 16	

Table 33

Pivot Table for Age Group (Survey Q1) and RQ3 (Survey Q10)

Years of age	Harshest of penalties	More than moderate penalties	Moderate penalties	Minimal to less than moderate penalties	No penalties
18 to 29	0.0%	4.1%	4.9%	0.0%	0.0%
30 to 39	5.5%	14.3%	29.5%	57.1%	25.0%
40 to 49	30.9%	33.7%	29.5%	28.6%	0.0%
50 to 59	38.2%	34.7%	26.2%	14.3%	75.0%
60 and up	25.5%	13.3%	9.8%	0.0%	0.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

There is a statistically significant relationship between *Survey Q5*: Technical Hacking Ability and *Survey Q10*: On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it would be implemented globally? The chi-square statistical results for technical hacking ability and RQ3: X^2 (4, N = 223) = 24.7, p = .0000583

The chi-square statistical analysis and a pivot table showing the descriptive statistics are provided (Tables 34-36).

Table 34

Chi-square Test on Technical Hacking Ability (Survey Q5) and RQ3 (Survey Q10)

	Basic	Advanced
Statistical significance (P-Value)	Very clearly significant	0.0000583
Effect Size (Cramér's V)	Medium	0.333

Note. Sample Size 223.

Table 35

Chi-squared Results

Chi square 24.7
Degrees of freedom 4

Table 36

Pivot Table for Hacking Ability (Survey Q5) and RQ3 (Survey Q10)

Technical hacking ability	Harshest of penalties	More than moderate penalties	Moderate penalties	Minimal to less than moderate penalties	No penalties
Technical hacking ability	20.8%	48.0%	65.6%	57.1%	75.0%
No technical hacking ability	79.2%	52.0%	34.4%	42.09%	25.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

There is a subtle but statistically significant relationship between *Survey Q3*: Gender and *Survey Q8*: On a scale from 1 to 5 please indicate how would you rate your attitude toward the need for one international law for defining criminal hacking? The chi-square statistical results for the gender and RQ1: X^2 (4, N = 225) = 12.2, p = .0158

The chi-square statistical analysis and a pivot table showing the descriptive statistics are provided (Tables 37-39).

Table 37

Chi-square Test on Gender (Survey Q3) and RQ1 (Survey Q8)

	Basic	Advanced
Statistical significance (P-Value)	Very clearly significant	0.0158
Effect size (Cramér's V)	Small	0.234

Note. Sample Size 225.

Table 38

Chi-squared Results

Chi square 12.2
Degrees of freedom 4

Table 39

Pivot Table for Gender (Survey Q3) and RQ1 (Survey Q8)

Gender	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree
Female	34.6%	16.3%	21.4%	28.6%	0.0%
Male	65.4%	83.8%	78.6%	71.4%	100.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

Summary

In this study I explored the relationships between the group of employment sector individuals, independent variables of age, ethnicity, gender, critical infrastructure affiliation, technical hacking ability, education level, and the dependent variables, which included the attitudes toward an international law for defining criminal hacking, the attitudes toward the need for the penalties of criminal hacking to be addressed under one international law, and the attitudes toward the extent that criminal hacking should be penalized, given it would be implemented globally.

The following research questions for the study were statistically analyzed, revealing no significant association between the groups of employment sector individuals and the independent and dependent variables of the study. RQ1: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for one international law for defining criminal hacking between public and private sector entities?, RQ2: Do age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education predict the attitudes toward the need for the penalties of criminal hacking to be addressed under

one international law between public and private sector individuals?, and RQ3: Is there a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on the attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties between public and private sector individuals?

The analysis from the chi-square tests showed no significant differences in the mean of the employment sector groups, which included public and private sector individuals, and the mean of the independent and dependent variables of the study. The null hypotheses for RQ1, RQ2, and RQ3 were statistically tested using a 95% confidence interval. Concerted efforts were taken to help ensure the correct inferences were gained and there were no type I or type II errors. The assumptions for the hypotheses testing included the level of measurement of the variables, the sampling method, the shape of the population distribution, and the sample size.

Although, there were no statistical significance among the research questions for the study, some statistical significance was found from analyzing the independent and dependents variables of the study, without the group of employment sector as the primary independent variable. The findings from these data analyses included: there is a statistical significance in age group and the attitudes toward the need for one international law for defining criminal hacking (RQ1), there is a statistical significance in age group and the attitudes toward the extent criminal hacking, as defined from the example in the study needs modification of stricter or lesser penalties (RQ3), there is a statistical significance in gender and the attitudes toward the need for one international law for

defining criminal hacking (RQ1), there is a statistical significance in infrastructure affiliation and the attitudes toward the extent criminal hacking, as defined from the example in the study (RQ3), and there is a statistical significance in hacking ability and the attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties (RQ3).

Through the data analyses, these data demonstrated the need for an international law for defining criminal hacking and the penalties associated with the crime, as well as to what extent the crime should be penalized, according to what is put forth and described in the United States CFAA, as an example for capturing respondent attitudes of lesser or more strict penalties. The theoretical approach used in the study illustrated how role theory and empathy have a connection in propelling effective policy employment for the future of criminal hacking laws at the international level. Chapter 5 concludes the study with interpretations of the findings, limitations, recommendations, and implications of the study.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this quantitative dissertation was to explore the relationship between individuals in the public and private sectors and their attitudes toward the need for one international law defining criminal hacking and the penalties associated with the act. The threat landscape in the virtual realm continues to escalate, leaving paths of destruction. The privacy and security of individuals, businesses, and global communities are suffering from the damages caused by criminal hacking.

I conducted this study hoping to find a relationship among the groups of the employment sectors, which included public and private sector individuals, and their attitudes on the need for an international law defining criminal hacking, attitudes toward the need for penalties for criminal hacking under one international law, and attitudes toward the extent criminal hacking, as defined from the example in the study, needs modification of stricter or lesser penalties. I hope this study will help propel solutions for answering and addressing these questions.

Summary of Key Findings

There were no significant associations between the groups of employment sector individuals and the independent and dependent variables of the study. Although there were no significant findings for the precise research questions of the study, there were findings of statistical significance found from analyzing the independent and dependent variables. Without the group of employment sector as the primary independent variable, a deeper dive into the relationships among the independent variables of age group,

infrastructure affiliation, gender, and hacking ability, and the dependent variables served the questions of the study.

The findings from these data analyses included the following statistical correlations. There is a statistical significance in age group and attitudes toward the need for one international law defining criminal hacking (Tables 22 and 23). There is a statistical significance in age group and attitudes toward the extent criminal hacking, as defined in the study, needs modification of stricter or lesser penalties (Tables 26 and 27). There is a subtle, but statistical, significance in gender and the attitudes toward the need for one international law defining criminal hacking (Tables 30 and 31). There is a strong statistical significance in infrastructure affiliation and attitudes toward the extent criminal hacking, as defined in the study, needs modification of stricter or lesser penalties (Tables 24 and 25). Lastly, there is a statistical significance in hacking ability and attitudes toward the extent criminal hacking, as defined in the study, needs modification of stricter or lesser penalties (Tables 28 and 29).

In retrospect, my study could have focused on fewer variables and eliminated employment sector as the overarching variable to be statistically analyzed among the independent and dependent variables. If the focus of the independent variable of groups, which included public sector and private sector individuals, was eliminated and the study proceeded with the remaining variables, the study would have shown statistically significant results and the null hypotheses for RQ3 would have been rejected and the alternative hypothesis accepted, showing a difference among age groups, ethnicity, gender, infrastructure sector affiliation, technical hacking ability, and education on

attitudes toward the extent criminal hacking, as defined from the examples in the study, needs modification of stricter or lesser penalties. The preceding alternative hypothesis excluded the groups of public and private sector individuals, as depicted in the study, as an example.

Interpretation of the Findings

The findings of my study align with the need to help curtail the damage being done on a global scale from activities of criminal hacking through the overwhelming responses toward the need to have more than moderate penalties for criminal hacking (Table 13). Bartholomae (2017) illustrated, through a network model comprising of a cloud service provider, consumers of the cloud service provider, and one who penetrates the cloud network to gain information, that global policy is needed to deter hacking by imposing higher fines. This can be applicable to the general consensus of the study for the penalties associated with criminal hacking. The survey responses, weighing more toward the attitude that the penalties for criminal hacking should be more than what are presently in place in the United States. The international community has made some gains since the 2001 treaty on cybercrime was implemented, although much more work is needed (Bartholomae, 2017).

Similarly, Visher and Weisburd (1998) expounded on how there needs to be tailored approaches for crime prevention strategies to help ensure recidivism rates decrease and are potentially alleviated. These approaches should involve efforts among stakeholders in establishing and implementing unique programs with precise elements for addressing specific types of crimes (Visher & Weisburd, 1998). By addressing criminal

hacking through a government role approach, while embodying empathy in the processes, governments, businesses, and organizations, as well as individuals, globally can reap the benefits of a stable global cyber realm. With leaders worldwide taking a holistic approach in using a lens that captures the threat landscape, privacy and security, and effective policies and laws, international legislative bodies can move forward collectively in helping to decrease criminal hacking levels.

The findings in this study confirm a need for policies to be addressed at the international level (Tables 9 and 11). Trotta (2017) elucidated the need for expert technocrat knowledge and the knowledge of the citizenry to help enhance policy efforts. The opinions of multidisciplinary experts and the population as a whole would greatly benefit from efforts being put forth in addressing criminal hacking policy solutions; everybody is being affected by the devastations created globally from criminal hacking. If these additional objectives were adopted as best practices and promulgated within the legislative realm around the world, there could be an increase in the rate at which critical policy issues are addressed in general.

Limitations of the Study

There were some limitations and a delimitation to my study. One limitation included a lack of previous studies in the research topic area, which made it harder to find studies that would provide meaning to the concepts of my study. Although the virtual realm has existed for decades, there have been few studies on the policy issues involving criminal hacking. This element presented challenges for building on the research of other studies involving the concepts, in relation to criminal hacking, the threat landscape,

security, privacy, policy, and laws, which were addressed in Chapter 2. Other limitations of the study, which are common for many research studies, were time and monetary resources. With unlimited time and money, the aims, goals, and outcomes of the study would have produced additional insights through the potential of a larger global sample size, providing additional data to be analyzed.

The data collection method could have been improved with more experience in collecting primary data. Experience in data collection may have helped in alleviating the additional amount of time involved in conducting the research study. Additionally, experience in data collection may have helped me bring in a larger sample size in a shorter amount of time, which would have potentially generated additional correlations or results for the study.

A delimitation of my study can be seen through too narrow of a research aim for the groups of the study, involving employment sectors, as the main focus of the study in relation to the independent variables and the dependent variables. This more narrowed approach eliminated the opportunity to gain statistical significance in other areas between the independent and dependent variables of the study. Fewer independent variables, while broadening the focus of the study in eliminating the primary independent variable of employment sector groups, would have allowed for the main focus of the study to be on examining the relationships between fewer independent variables and the dependent variables of the study, providing for additional correlations for the questions of the study.

Recommendations and Future Studies

Criminal hacking touches numerous entities worldwide from individuals, companies, organizations, and governments, to name a few. A theme I uncovered, throughout the research process, is how prevalent hacking is internationally. There has been a rise in information warfare, stated Lei (2019), which involves gaining an advantage from the use of information. The use of information to gain an advantage has been taking place globally, with a few countries being noted on the news front as being more active in this area. The U.S. Justice Department indicted four Chinese hackers in the Equifax breach in February 2020 (Dufner, 2020). It is unknown if there will be any resolutions from these indictments. Marks (2019) suggested that hackers of North Korea have been using information warfare technics, although their acts are seen by many as acts of espionage, rather than criminal hacking acts. With no clear definition for criminal hacking, gray areas pertaining to criminal hacking and information warfare continue to be an issue in the policy realm, with a great deal of work yet to be done in establishing a framework that clearly addresses criminal hacking holistically.

Scharf and Taylor (2017) showed how the crime of piracy, an international crime over two hundred years old, could offer some new perspectives on addressing similar issues in modern day societies. It has been suggested we look at the international laws of piracy for building a coordinative framework for addressing cybersecurity related issues in relation to computer intrusions (Lei, 2019; Shackelford, 2017a). Scholars could study the viability of using an existing international framework, under international law and piracy, to address the criminal acts of hacking in future studies.

Additional insights could be gained from the hacking culture today, toward policy solutions in the criminal hacking realm, through future scholarly studies anonymously involving todays, more transparent, technological hackers and whether age group, ethnicity, and gender plays a part in differentiating opinions. Hiltner, a reporter for the Surfacing column (September 2018), showed how some anonymity and privacy perceptions are moving in a different direction from what was once considered to be the norm of only using aliases, which can be seen through interactions from hacker conferences, such as the annual hacking conference held in Las Vegas, Nevada, Defcon. Hiltner illustrated how the pressures involving demands by the private and public sectors for experts in the cybersecurity field and bug bounty programs, propelled by professional entities and the gamification arena, have shown a present day need for various aspects of the hacking culture (Hiltner, 2018).

Similar to my study, I recommend future studies, which could offer additional insights for addressing policy issues in the criminal hacking realm and if there should be policies at the international level, solely studying the attitudes of technological hackers. These future studies, addressing the attitudes of those with technological hacking skills and if their attitudes reveal there is a need for international laws addressing criminal hacking, could provide policy solutions that have not yet been considered. The information gained by these future studies could be used by international legislative bodies for helping to determine the scope of criminal hacking laws on an international level.

Political culture in relation to an international framework addressing criminal hacking could pose as a future study involving a sample of the legislative population in a number of countries. The study could offer a great deal of insight as to how international communities should move forward in holistically addressing criminal hacking and if one international law is feasible, providing the vast differences in political cultures around the world. This study could also be used in concert with meta-analysis for studying various populations around the world and their attitudes on an international framework for criminal hacking. Singh (2007) showed how meta-analysis is used to find patterns from multiple studies, using a number of statistical tests, to help in solving research problems.

Scholars could gain additional insights from future studies involving global government leaders on if there is a need for an international law for defining criminal hacking, policies associated with criminal hacking, and what penalties should be attributed for committing the crime. The results of this future study potentially could add to the findings of my study and other studies, in the criminal hacking realm, for determining if there are additional outliers that should be considered for the development of international laws and policies, in general, for addressing criminal hacking policies among international communities. A multidisciplinary approach in gaining insights from future studies for international policy development in the criminal hacking realm should help escalate potential policy solutions for addressing universal criminal hacking policy issues.

Finally, a future study, limited to a few independent variables, without the inclusion of employment sector groups, as my study included, could be employed so data

from a larger global sample could be analyzed to see if there is a significance among the variables of the study and the attitudes toward the penalties of criminal hacking and international laws. Promoting future scholarly studies in the realm of criminal hacking and policy development will help ensure there are ample amounts of data to sift through in efforts to find beneficial correlations that could have a positive impact on the trajectory of future laws for criminal hacking.

Implications

There are some implications for positive social change in the policy realm, which would ultimately have an impact on every member of the global society, as a whole. Callahan et al. (2012) illustrated a multifaceted framework that Walden University has used for a number of social change initiatives stemming from the Walden University community of alumni, faculty members, and students. The framework included a number of features that potentially could be webbed together to provide a holistic approach to addressing positive social change in a number of areas among our global communities. The framework consists of eight features that involve collaboration, advocacy, practice, civic engagement, humane ethics, systematic thinking, scholarship, and reflection (Callahan et al., 2012).

The elemental framework Callahan et al. (2012) depicted would work very well in promoting future studies in the realm of cybersecurity and ultimately providing for a holistic policy development approach for defining criminal hacking internationally, and the penalties that should be associated with the crime. The pieces of collaboration and advocacy (Callahan et al., 2012) are instrumental, in that collaboration is needed at all

levels of government for addressing criminal hacking and advocacy is needed in attempts to propel the policy initiatives. Scholarship, systematic thinking, civic engagement, and practice, additional pieces of the Callahan et al. (2012) framework, culminate into a practitioner's model that could be used to further the initiatives already in place in the cybersecurity realm, for holistically using a team approach that embodies the great minds of today for actively solving the modern-day issues of criminal hacking and effective policy implementation. Finally, the key elements described, as well as the additional elements of humane ethics and reflection, from the features of the Callahan et al. (2012) framework, are needed to fully capture a holistic approach for addressing the needs of humanity in the ever evolving threat landscape of criminal hacking, including the culture that brings these criminal acts to fruition.

Building a framework consisting of agreements, rules, and laws among international bodies is paramount in protecting societies and today and in the future from the adverse and damaging effects of criminal hacking. Concerted efforts among technical experts, including the hacking community, and the legislative realm will help propel policy solutions for criminal hacking. An awareness approach, as to the hazards of criminal hacking, could bring forth even more concerted efforts on a multidisciplinary plane for finding answers to the policy issues we face today. Dissuading the criminal hacking culture could pose as an additional approach in moving forward toward a policy solution that captures the best interests of the entire global population.

Conclusion

In summary, the examination of the attitudes of individuals, across the public and private employment sectors, provided a general consensus, according to 82 percent of survey respondents, on the need for an international law for defining criminal hacking, the need for an international law for criminal hacking, according to 80 percent of survey respondents, and addressing the penalties for criminal hacking at a standard that would be more intense than what is put forth in the United States CFAA, according to 68 percent of survey respondents. The deficiencies in clear policies being addressed across multinational jurisdictions has enabled for lines to be blurred in what is deemed as criminal hacking, the true origins of the intrusions, and a codification for bringing those responsible for the economically and culturally crippling acts of criminal hacking. An expansion of concerted efforts among multidisciplinary experts in the fields of the threat landscape of the cyber realm, security and privacy, policy and law, and the hacking culture, as a whole, may help contribute to effective policy solutions for addressing the major dilemma we are facing involving the harmful trickling effects of criminal hacking. Present day global entities and the future support of humankind depends on an effective approach for curtailing the nefarious acts and disastrous effects of criminal hacking worldwide.

References

3D printing is vulnerable to hackers. (2016). *The Chemical Engineer, 903*, 16. Retrieved from https://www.thechemicalengineer.com/

10 Questions with Derek Brink. The weakest link in computer security is humans. (2003). *Journal of Financial Planning, 16*(4), 14–22. Retrieved from https://www.onefpa.org/journal/Pages/default.aspx

$500. (2017). *Government technology, 30*(4), 53. Retrieved from https://www.govtech.com/

Ablon, L., & Libicki, M. (2015). Hackers' Bazaar: The markets for cybercrime tools and stolen data. *Defense Counsel Journal, 82*(2), 143–152. doi:10.12690/0161-8202-82.2.143

Absolute Software Corporation. (2016, February 19). Absolute survey: One-third of IT managers admit to hacking. *ENP Newswire*. Retrieved from http://www.enpublishing.co.uk/ENPN.htm

Adigbuo, R. (2007). Beyond IR theories: The case for national role conceptions, *Politikon, 34*(1), 83–97. doi:10.1080/02589340701336286

Al-khateeb, S., Conlan, K. J., Agarwal, N., Baggili, I., & Breitinger, F. (2016). Exploring deviant hacker networks (DHN) on social media platforms. *Journal of Digital Forensics, Security & Law, 11*(2), 7–20. doi:10.15394/jdfsl.2016.1375

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1/2), 643–656. Retrieved from https://www.cybercrimejournal.com/

Banks, W. (2017). State responsibility and attribution of cyber intrusions after Tallinn 2.0. *Texas Law Review, 95*(7), 1487–1514. Retrieved from https://texaslawreview.org/

Banks, W. C. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory Law Journal, 66*(3), 513–525. Retrieved from https://law.emory.edu/elj/

Barnes, J., Conrad, K., Demont-Heinrich, C., Graziano, M., Kowalski, D., Neufeld, J., … Palmquist, M. (1994–2012). Generalizability and transferability. Writing@CSU. Colorado State University. Retrieved from https://writing.colostate.edu/guides/guide.cfm?guideid=65.

Bartholomae, F. (2018). Cybercrime and cloud computing. A game theoretic network model. *Managerial & Decision Economics, 39*(3), 297–305. doi:10.1002/mde.2904

Below, A. (2014, December 5). *Environmental politics and foreign policy decision making in Latin America: Ratifying the Kyoto Protocol*. New York, NY: Routledge.

Bencie, L. (2012). International hotel rooms: The enemy's gateway to economic and industrial espionage. *Journal of Counterterrorism & Homeland Security International, 18*(1), 10–12. Retrieved from https://www.ebsco.com/products/research-databases/international-security-counter-terrorism-reference-center

Bengtsson, R., & Elgström, O. (2012). Foreign policy analysis, conflicting role

conceptions? *The European Union in Global Politics, 8*, 93–108. Retrieved from https://doi.org/10.1111/j.1743-8594.2011.00157.x

Bento, A., & Bento, R. (2004). Empirical test of a hacking model: An exploratory study. *Communications of the Association for Information Systems, 14*. doi:10.17705/1cais.01432

Birkland, T. A. (2016). *An introduction to the policy process: Theories, concepts, and models of public policy making* (4th ed.). Abingdon, United Kingdom: Routledge.

Bonner, K. (2016). Arendt, role theory and the ethical evaluation of action. *Irish Journal of Sociology, 24*(2), 200–225. doi:10.7227/ijs.0007

Boston Global Forum. Retrieved from http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/

Bradbury, D. (2011). Hacking Wi-Fi the easy way. *Network Security, 2011*(2), 9–12. doi:10.1016/S1353-4858(11)70014-9

Brown, G., & Poellet, K. (2012). The customary international law of cyberspace. *Strategic Studies Quarterly, 6*(3), 126–145.

Buchanan, B. (2016). *The cybersecurity dilemma*. Oxford, United Kingdom: Oxford University Press.

Burkart, P., & McCourt, T. (2017). The international political economy of the hack: A closer look at markets for cybersecurity software. *Popular Communication, 15*(1), 37. doi:10.1080/15405702.2016.1269910

Callahan, D., Wilson, E., Birdsall, I., Estabrook-Fishinghawk, B., Carson, G., Ford, S., & Yob, I. (2012). Expanding our understanding of social change [Report].

Baltimore, MD: Walden University

Castelluccio, M. (2017). The most notorious hacks of 2016. *Strategic Finance, 55*. Retrieved from https://sfmagazine.com/post-entry/january-2017-the-most-notorious-hacks-of-2016/

Cavelty, M. D., & Mauer, V. (2013). *Power and security in the information age: Investigating the role of the state in cyberspace*. Abingdon, United Kingdom: Routledge.

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders, 11*(4), 534–555, doi:10.1080/15564886.2015.1121944

Cordell, C. (2018, November 9). Air Force wants a better view of the landscape for intelligence analytics tools. *Fedscoop.* Retrieved from https://www.fedscoop.com/afrl-wants-better-view-of-the-landscape-for-intelligence-analytics-tools/

Creswell, J. W. (1994). *Research design: Qualitative and quantitative approaches*. Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2016). Reflections on the MMIRA the future of mixed methods task force report. *Journal of Mixed Methods Research, 10*(3), 215–219. doi:10.1177/1558689816650298

Cusumano, M. A., & Yoffie, D. B. (2016). Extrapolating from Moore's Law.

Communications of the ACM, 59(1), 33–35. doi:10.1145/2846084

DeBenedictis, E. P. (2017). It's time to redefine Moore's Law again. *Computer, 50*(2), 72–75. doi:10.1109/MC.2017.34

Denning, P. J. (1983). Editorial: Moral clarity in the computer age. *Communications of the ACM, 26*(10), 709–710. doi:10.1145/358413.358415

Denning, P. J., & Lewis, T. G. (2017). Exponential laws of computing growth. *Communications of the ACM, 60*(1) 54–65. doi:10.1145/2976758

Din, M. F. (2015). Breaching and entering. *Brooklyn Law Review, 81*(1), 405–440. Retrieved from https://brooklynworks.brooklaw.edu/blr/

Dixon, B. (2007). IT security: Moving beyond technology toward policy and education. *PA Times, 30*(5), 3–1. Retrieved from https://patimes.org/

Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders, 11*(4), 556–577. doi:10.1080/15564886.2016.1173157

Dufner, E. (2020). Justice Department Indicted 4 Chinese Hackers in Equifax Breach. Bloomberg.Com, N.PAG. Retrieved from https://www.bloomberg.com/businessweek

Dupont, B., Côté, A., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129–151. doi:10.1080/17440572.2016.1157480

Edge, M. (2016). *Political philosophy, empathy, and political justice*. New York, NY: Routledge.

Elkin-Korerd, N., & Haber, E. (2016). Governance by Proxy. *Brooklyn Law Review*,

82(1), 105-162.

Encryption breaking quantum computers getting closer, warns Canadian expert. (2017, September 13). *IT World Canada*. Retrieved from http://www.itworldcanada.com/article/encryption-breaking-quantum-computers-getting-closer-warns-canadian-expert/396496

Fidler, D. P. (2016). Cyberspace, terrorism and international law. *Journal of Conflict & Security Law*, 21(3), 475–493. Retrieved from https: //doi-org.ezp.waldenulibrary.org/10.1093/jcsl/krw013

Garris, J. (2017). There's no going it alone: Disrupting major cybercrime rings (a Case Study). *ISSA Journal,* 15(4), 20-47. Retrieved from https://www.issa.org/journal/

Gewirtz, D. (2011). Game-changing threat: The rise of the hacking collective. *Journal of Counterterrorism & Homeland Security International,* 17(3), 6. ISSN:1552-5155

Gewirtz, D. (2013). Worse nightmare: New ways emergency communications can be disrupted by hackers and terrorists. *Journal of Counterterrorism & Homeland Security International,* 19(2), 8-10. Retrieved from Retrieved from https://www.ebsco.com/products/research -databases/international-security-counter-terrorism-reference-center

Gewirtz, D. (2015). Iran and LinkedIn: Using this social career site-as an entry point to critical infrastructure attacks. *Journal of Counterterrorism & Homeland Security International,* 21(3), 8-9. Retrieved from https://www.ebsco.com/products/research -databases/international-security-counter-terrorism-reference-center

Gerwitz, D. (2016). How bad guys are using the web's own encryption to hide malware payloads. *Journal of Counterterrorism & Homeland Security International*, 22(1), 8-10. Retrieved from https://www.ebsco.com/products/research -databases/international-security-counter-terrorism-reference-center

Ghappour, A. (2017). Searching places unknown: law enforcement jurisdiction on the dark web. *Stanford Law Review*, (4), 1075. Retrieved from https://www.stanfordlawreview.org/

Ghernaouti, S. (2013). Cyber power – crime, conflict and security in cyberspace. Lausanne, Switzerland: EPFL Press.

Global Forum on Cyber Expertise (2017, November). A decade of IGF: Achievements and challenges ahead. *Global Cyber Expertise Magazine, 2* (Global Technologies), 32-33. Retrieved from https://www.thegfce.com/about/magazine doi:10.1145/2063176.2063184

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705. Doi: 10.2501/IJMR-2017-050

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. New York, NY: Doubleday.

Gold, S. (2012). Hacking on the hoof. Engineering & Technology (17509637), 7(3), 80-83. doi:10.1049/et.2012.0313

Greengard, S. (2012). Law and disorder. *Communications of the ACM*, 55(1), 23-25. doi:10.1145/2063176.2063184.

Gupta, P., & Mata-Toledo, R. (2016). Cybercrime: In disguise crimes. *Journal of Information Systems & Operations Management,* 1-10. Retrieved from http://www.sciencepublishinggroup.com/journal/index?journalid=104

Hacking the House: Chapter 1 - The Chicago doorbell. (2016). IEEE Consumer Electronics Magazine, Consumer Electronics Magazine, IEEE, *IEEE Consumer Electron. Mag,* (1), 81. doi:10.1109/MCE.2015.2484741

Hacking the House Chapter 2: The Boston VoIP doorbell. (2016). IEEE Consumer Electronics Magazine, Consumer Electronics Magazine, IEEE, *IEEE Consumer Electron. Mag*, (2), 44. doi:10.1109/MCE.2016.2516078

Hacking the House Chapter 3: Nonstop Internet. (2016). IEEE Consumer Electronics Magazine, Consumer Electronics Magazine, IEEE, *IEEE Consumer Electron. Mag,* (4), 68. doi:10.1109/MCE.2016.2590179

Hacking Smart Parking Meters. (2016). 2016 International Conference on Internet of Things and Applications (IOTA), Internet of Things and Applications (IOTA), International Conference on, 191. doi:10.1109/IOTA.2016.7562720

Hathaway, M. E. (2014). Connected choices: How the internet is challenging sovereign decisions. *American Foreign Policy Interests*, 36(5), 300-313. doi:10.1080/10803920.2014.969178

Hampson, N. N. (2012). Hacktivism: A new breed of protest in a networked world. *Boston College International & Comparative Law Review*, 35(2), 511-542. Retrieved from https://lawdigitalcommons.bc.edu/iclr/

Heikkila, F. L. (2009). An Analysis of the Impact of Information Security Policies on

Computer Security Breach Incidents in Law Firms. (Doctoral). United States: Nova Southeastern University. Davie.

Hausken, K. (2017). Security investment, hacking, and information sharing between firms and between hackers. *Games* (20734336), 8(2), 1-23. doi:10.3390/g8020023

Hill, J. B. & Marion, N. E. (2016). Introduction to cybercrime: Computer crimes, laws, and policing in the 21st Century. Westport, CT: Praeger Security International.

Hiltner, S. (2018, September 22). For hackers, anonymity was once critical. That's changing. *New York Times*, Retrieved from http://www.nytimes.com

Hooker, M., & Pill, J. (2016). You've been hacked, and now you're being sued: The developing world of cybersecurity litigation. *Florida Bar Journal*, 90(7), 30-40. Retrieved from https://www.floridabar.org/the-florida-bar-journal/

How Businesses Can Speed Up International Cybercrime Investigation. (2017). IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Security. *Privacy,* (2), 102. doi:10.1109/MSP.2017.40

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A Survey. *ACM Computing Surveys*, 51(4), 1–36. doi:10.1145/3199674

Hui, K., Kim, S. H., & Wang, Q. (2017). Cybercrime deterrence and international legislation: Evidence form distributed denial of service attacks. *MIS Quarterly*, 41(2), 497-A11. Retrieved from https://misq.org/archive/

Hunsinger, J., & Schrock, A. (2016). The democratization of hacking and making. *New Media & Society*, 18(4), 535-538. doi:10.1177/1461444816629466

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity. *Ethics & Information Technology*, 18(2), 117-129. doi:10.1007/s10676-016-9398-9

Ihantola, E., & Kihn, L. (2011). Threats to validity and reliability in mixed methods accounting research. *Qualitative Research in Accounting & Management*, 8(1), 39.

International Law - Universal Jurisdiction - United Kingdom Adds Barrier to Private Prosecution of Universal Jurisdiction Crimes. Police Reform and Social Responsibility Act, 2011, c. 13 (U.K.). (2012). *Harvard Law Review*, 1251554

Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R., & Engel, T. (2015). Car hacking experiment: When connectivity meets vulnerability. 2015 IEEE Globecom Workshops. doi:10.1109/glocomw.2015.7413993

Kain, R. C. (2013). Federal computer fraud and abuse act: Employee hacking legal in California and Virginia, but illegal in Miami, Dallas, Chicago, and Boston. *Florida Bar Journal*, 87(1), 36-39. Retrieved from https://www.floridabar.org/the-florida-bar-journal/

Kanji, G. K. (2006). 100 statistical tests. London, SAGE Publications Ltd doi: 10.4135/9781849208499

Kennedy, G., & Xiaoyan, Z. (2017). China passes cybersecurity law. *Intellectual Property & Technology Law Journal*, 29(3), 20-21. Retrieved from https://www.usfca.edu/law/professional-skills/student-run-academic-journals/iptlj

Kosseff, J. (2017). Cybersecurity law. Retrieved from https://ebookcentral.proquest.com

Lanz, J., & Cohen, N. A. (2012). Protecting privacy. *Journal of Accountancy*, 214(2), 22. Retrieved from https://www.journalofaccountancy.com/

Lei, H. (2019). Modern information warfare: analysis and policy recommendations. *Foresight,* 21(4), 508–522. doi:10.1108/FS-06-2018-0064.

Lindqvist, U., & Neumann, P. G. (2017). The future of the internet of things. *Communications of The ACM*, 60(2), 26-30. doi:10.1145/3029589

Madarie, R. (2017). Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology,* 11(1), 78–97. Retrieved from http://doi.org/10.5281/zenodo.495773

Marks, J. (2019). The Cybersecurity 202: North Korea's hackers accused of blurring lines between spies and criminals. *The Washington Post*. Retrieved from https://www.washingtonpost.com/

Mansfield-Devine, S. (2014). Hacking on an industrial scale. Network Security, 2014(9), 12-16. doi:10.1016/S1353-4858(14)70092-352.

McDonald, S. H. (2002). Globalization and risk: A contingent response for democratic governance. Administrative Theory & Praxis (Administrative Theory & Praxis), 24(1), 31. doi:10.1080/10841806.2002.11029347.

McMillan, R. (2009). As hacking hits home, China strengthens cyber laws. *Computerworld Hong Kong,* 26(5), 74. Retrieved from https://www.cw.com.hk

McQuade, S.C III. (2006). Understanding and Managing Cybercrime, Pearson.

Mendelson, D., & Mendelson, D. (2017). Dossier Privacy: Definition, protection and projection: Legal protections for personal health information in the age of Big

Data – a proposal for regulatory framework. Ethics, *Medicine and Public Health,* 337-55. doi:10.1016/j.jemep.2017.02.005

Menon, S. & Siew, T. G. (2012). Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation, *Journal of Money Laundering Control,* 15(3) pp. 243-256. doi:10.1108/13685201211238016

Mertens, D. M. & Hesse-Biber, S. (2012, May). Triangulation and mixed methods research provocative positions. *Journal of Mixed Methods Research*, May 2012. doi:10.1177/1558689812437100

Mihai, I. C., Pruna, S. S., & Petrica, G. G. (2017). A comprehensive analysis on cyber-threats against elearning systems. *Elearning & Software for Education*, 3344-351. doi:10.12753/2066-026X-17-225

Mikhaylov, A., & Frank, R. (2016). Cards, money and two hacking forums: An analysis of online money laundering schemes. 2016 European Intelligence and Security Informatics Conference (EISIC). doi:10.1109/EISIC.2016.021

Mitchell, C. (2016). Hacked: The inside story of America's struggle to secure cyberspace. Lanham, MD: Rowman and Littlefield.

Mills, C. (1992). Values and public policy. San Diego, CA: Harcourt Brace Jovanovich College Publishers.

Morse, J. M., Niehaus, L., Wolfe, R. R., & Wilkins, S. (2006). The role of the theoretical drive in maintaining validity in mixed-method research. *Qualitative Research in Psychology*, 3(4), 279-291. Retrieved from https://www.tandfonline.com/loi/uqrp20

Nash, E., & Thomas, D. (2006). Worldwide laws fail to fight cybercrime. *Computing* (13612972), 8. Retrieved from https://www.springer.com/journal/607

Newman, E., Thakur, R., Tirman, J. (2006). Multilateralism under challenge? Power, international order, and structural change. Tokyo, Japan: United Nations University Press.

Oh, S. & Lee, K. (2014). The need for specific penalties for hacking in criminal law. *The Scientific World Journal*, Retrieved from http://dx.doi.org/10.1155/2014/736738

Öhlén, J. (2011). Mixed method design: Principles and procedures. *Forum: Qualitative Social Research*, 12(1), 1-8. Retrieved from https://doaj.org/toc/1438-5627

Osborne, J. (2008). Best practices in quantitative methods. Thousand Oaks, CA: SAGE Publications. doi:10.4135/9781412995637

Osborne, J. W. (2017). Best practices: A moral imperative. Canadian Journal of Behavioural Science / Revue Candienne Des Sciences Du Comportement, 49(3), 153-158. doi.10.1037obs0000078

Pollaro, G. (2010). Disloyal computer use and the computer fraud and abuse act: Narrowing the scope. *Duke Law & Technology Review,* (11/12), 1-11. Retrieved from https://scholarship.law.duke.edu/dltr/vol16/iss1/

PR N. (2017, July 5). LOGICFORCE Report finds 40% of law firms were unaware they were breached in 2016. PR Newswire US. Retrieved from https://www.prnewswire.com/news-releases/logicforce-report-finds-40-of-law-firms-were-unaware-they-were-breached-in-2016-300483518.html

Pogue, C. (2018). The black report: Decoding the minds of hackers. Nuix Software

Company. Retrieved from https://www.nuix.com/search?query=black+report+2018

Privacy Preserving in Banking Sector. (2016). 2016 2nd international conference on applied and theoretical computing and communication technology (iCATccT), 2016 2nd International Conference on, 571. doi:10.1109/ICATCCT.2016.7912065

Pun, D. (2017). Rethinking espionage in the modern era. *Chicago Journal of International Law*, (1), 353. Retrieved from https://chicagounbound.uchicago.edu/cjil/

Qualtrics, Determining Sample Size: How to Ensure You Get the Correct Sample Size. Retrieved from https://www.qualtrics.com/experience-management/research/determine-sample-size/

Qualtrics, Provo, UT. Statistical Software Version 2019 – 2020. www.qualtrics.comRaimondo, E., & Newcomer, K. E. (2017). Mixed-methods inquiry in public administration: The interaction of theory, methodology, and praxis. *Review of Public Personnel Administration*, 37(2), 183-201. doi:10.1177/0734371X17697247

Raosoft, Sample Size Calculator. (n.d.). Retrieved from http://www.raosoft.com/samplesize.html

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime tendencies and legislation in the Republic of Macedonia. *European Journal on Criminal Policy & Research,* 22(1), 127-151. doi:10.1007/s10610-015-9277-7

Reinis, U. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology,* 10(2), 127-146. doi:10.5281/zenodo.163393

Richmond, R., Morrison, K. M., & Covarrubias, K. J. (2017). Keeping your trade secrets secret. *Employee Relations Law Journal*, 43(2), 26-35. Retrieved from https://lrus.wolterskluwer.com/store/product/employee-relations-law-journal/

Riga, S. A. (2017). Two breaches, two enforcement actions, and a DDOS attack: Data security and the rise of the internet of things. *Journal of Internet Law*, 20(9), 3-7. Retrieved from https://www.researchgate.net/journal/1094-2904_Journal_of_Internet_Law

Roberts, K. V. (2013). Sun Tzu and the art of cyber warfare. *Journal of Counterterrorism & Homeland Security International*, 19(1), 12-14. Retrieved from https://www.ebsco.com/products/research-databases/international-security-counter-terrorism-reference-center

Sabett, R. V. (2016). Who's ready for a J.D.? *ISSA Journal*, 14(10), 7. Retrieved from https://www.issa.org/journal/

Sabett, R. V. (2017). (Not) the best of cybersecurity, 2016 version. *ISSA Journal,* 15(1), 5. Retrieved from https://www.issa.org/journal/

Scharf, M. & Taylor, M. (2017). A Contemporary Approach to the Oldest International Crime. *Utrecht Journal of International and European Law*, (84), 77.

Secretary-Generals' Report to Ministers, OECD, 2017. Retrieved from: http://www.oecd.org/

Schultze, S. J. (2016). Hacking immunity: computer attacks on United States territory by foreign sovereigns. *American Criminal Law Review*, (3), 861. Retrieved from *American Criminal Law Review*

Segura Serrano, A. (2015). Cybersecurity: Towards a global standard in the protection of critical information infrastructures. *European Journal of Law & Technology*, 6(3),1. Retrieved from http://ejlt.org/

Shackelford, S. J. (2017). Human Rights and Cybersecurity Due Diligence: A Comparative Study. *University of Michigan Journal of Law Reform*, 50(4), 859-885. Retrieved from https://repository.law.umich.edu/mjlr/

Shackelford, S. J. (2017). The law of cyber peace. *Chicago Journal of International Law*, (1), 1. Retrieved from https://chicagounbound.uchicago.edu/cjil/

Shackelford, S. J., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Craig Deckard, A. N., ... Smith, J. M. (2017). Making democracy harder to hack. *University of Michigan Journal of Law Reform*, 50(3), 629-668. Retrieved from Retrieved from https://repository.law.umich.edu/mjlr/

Sibona, C., & Walczak, S. (2012). Purposive sampling on twitter: A case study. 2012 45th Hawaii International Conference on System Sciences, System Science (HICSS), 2012 45th Hawaii International Conference On, 3510–3519

Singh, K. (2007). Quantitative Social Research Methods. SAGE Publications India Pvt Ltd.

Snell, R. (2016). The long-term impact of forced transparency. *Journal of Health Care Compliance,* 18(6), 3-4. Retrieved from

https://www.thefreelibrary.com/Journal+of+Health+Care+Compliance.-a0130629819

Söderberg, J., & Delfanti, A. (2015). Hacking hacked! The life cycles of digital innovation. *Science, Technology & Human Values,* 40(5), 793-798. doi:10.1177/0162243915595091

Solomon, S. (2020, Feb. 16). AI a new and frightening battlefield in cyber war, experts warn. *Times of Israel*. Retrieved from https://www.timesofisrael.com/ai-a-new-and-frightening-battlefield-in-cyber-war-experts-warn/

Sommer, P. (2006). Criminalising hacking tools. Digital Investigation, 3(2), 68–72. doi:10.1016/j.diin.2006.04.005

States Territory by Foreign Sovereigns. *American Criminal Law Review*, 53(3), 861-895.

Strategic Orientations of the Secretary-General, Meeting of the OECD Council at Ministerial Level, Paris, June 7-8, 2017.

Stone, A. (2012). Here's the catch. *Government Technology*, 25(7), 20-24. Retrieved from https://www.govtech.com/

Sullivan, C. (2015). The 2014 Sony hack and the role of international law. *Journal of National Security Law & Policy,* 8(3), 1-27. Retrieved from https://jnslp.com/

Tang, Z., Bagchi, K., & Jain, A. (2009). Explorative assessment of internet hacking: An agent-based modeling approach. *Journal of Information Privacy & Security*, 5(2), 42-64.

Taylor, P. A. (1999). Hackers: Crime in the digital sublime. London: Rutledge

Thaw, D. (2014). The efficacy of cybersecurity regulation. *Georgia State University Law Review,* 30(2), 287. Retrieved from https://readingroom.law.gsu.edu/gsulr/

The Day the Cryptography Dies. (2017). IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Security. *Privacy,* (4), 14. oi.10.1109/MSP.2017.315132

The Identity Theft Resource Center (n.d.). Retrieved from http://www.idtheftcenter.org/Data-Breaches/data-breaches

The Latest: US, China agree not to steal trade secrets. (2015, September 25). UWIRE Text, p. 1. Retrieved from https://www.uwire.com/

Theohary, C. A., & Rollins, J. (2009). Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress: R40836. Congressional Research Service: Report, 1-23.

Thies, C. G. (2009). Role theory and foreign policy. Retrieved from http://myweb.uiowa.edu/bhlai/workshop/role.pdf

Tomblin, J., & Jenion, G. (2016). Sentencing 'Anonymous': exacerbating the civil divide between online citizens and government. *Police Practice & Research*, 17(6), 507–519. doi:10.1080/15614263.2016.1205983

Trivun, V., Mahmutćehajić, F., & Silajdžić, V. (2012). Law and the internet revolution: The need for adjustment. Conference Proceedings: International Conference of The Faculty of Economics Sarajevo (ICES), 932-943

Trotta, A. (2017). Advances in E-Governance: Theory and application of technological initiative. New York: Routledge.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker.

International Journal of Cyber Criminology, 2(2), 382-396. Retrieved from https://www.cybercrimejournal.com/

U.S. Department of Homeland Security Privacy Office. (2002). Handbook for Safeguarding Sensitive Personally Identifiable Information. Revised in 2012. U.S. Department of Homeland Security Washington, DC: U.S. Government Printing Office.

Upol, A. K. (2014). G7 Summit Seals Putin's Pyrrhic Victory? *International Policy Digest,* 1(6), 43. Retrieved from https://intpolicydigest.org/

Van Der Walt, C. (2017). Feature: The impact of nation-state hacking on commercia l cyber-security. *Computer Fraud & Security*, 20175-10. doi:10.1016/S1361-3723(17)30030-1

Visher, C. A., & Weisburd, D. (1998). Identifying what works: Recent trends in crime prevention strategies. *Crime, Law & Social Change,* 28(3/4), 223-242. Retrieved from https://www.springer.com/journal/10611

Walton, B. A. (2017). Duties owed: low-intensity cyber-attacks and liability for transboundary torts in international law. *Yale Law Journal*, (5), 1460. Retrieved from https://www.yalelawjournal.org/

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence & National Security*, 27(5), 781-799. doi:10.1080/02684527.2012.7085

Weber, R. H. and Studer, E. (2016). Cybersecurity in the internet of things: Legal aspects. *Computer Law & Security Review*, October, (32) 5, 715-728. Retrieved from https://www.journals.elsevier.com/computer-law-and-security-review

Wehner, L. E., & Thies, C. G. (2014). Role theory, narratives, and interpretation: The domestic contestation of roles. *International Studies Review,* 16(3), 411-436. doi:10.1111/misr.12149

Wenzel, S. L. (2017). Not even remotely liable: Smart car hacking liability. *Journal of Law, Technology & Policy*, 2017(1), 49. Retrieved from http://illinoisjltp.com/journal/archives/

Wide Range of Devices Vulnerable to Hacking. (2015). Network Security, 2015(12), 20. doi:10.1016/S1353-4858(15)30114-8

Williams, B. R. (2017). Global Cyber Enforcement. *ISSA Journal*, 6. Retrieved from https://www.issa.org/journal/

Williams, T. C. (2015). Simple (cyber) sabotage. *Journal of Counterterrorism & Homeland Security International*, 21(1), 12-13. Retrieved from Retrieved from Retrieved from https://www.ebsco.com/products/research -databases/international-security-counter-terrorism-reference-center

Wilsem, J. v. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437-453. doi:10.1177/1043986213507402

Young, R., & Zhang, L. (2007). Illegal computer hacking: An assessment of factors that encourage and deter the behavior. *Journal of Information Privacy & Security,* 3(4), 33-52. doi:10.1080/15536548.2007.10855827

Appendix A: Alignment Table for Variables of the Study

	IV1: Age Group	IV2: Ethnicity	IV3: Gender	IV4: Infrastructure Affiliation	IV5: Technical Hacking Ability	IV6: Education	Group: Public Sector	Group: Private Sector
DV1: Attitudes towards the need for one international law for defining criminal hacking								
DV2: Attitudes towards the need for the penalties of criminal hacking to be addressed under one international law								
DV3: Attitudes towards the extent that criminal hacking should be penalized, given it would be implemented globally								

Appendix B: Survey

This virtually disseminated survey is anonymous and voluntary and all information provided will be used to fulfill the requirements for a research study dissertation involving an examination of attitudes towards international standards for criminal hacking. All answers are anonymous, including not capturing any IP addresses through the survey platform. One must be 18 years or older to participate in the survey.

Around the world there are a number of statements defining computer intrusions, or criminal hacking. Definitions include variations of some or all of the following: intentionally accessing a protected device without authorization or exceeding authorized access. There are also different standards, among various nations, that have been used for addressing the penalties for criminal hacking. This study will examine attitudes on whether there is a need for one international law that clearly defines criminal hacking and the penalties associated with the act.

1 – Age Group

Please select which age bracket you are in.

- 18 to 29 years of age
- 30 to 39 years of age
- 40 to 49 years of age
- 50 to 59 years of age
- 60 years of age and above

2 – Ethnicity

Please specify the ethnic origin you most closely align with.

- Asian descent
- African descent
- American descent
- Australian descent
- Canadian descent
- European Union descent
- Hispanic or Latino descent
- India national descent
- Middle Eastern descent
- Russian descent
- Other

3 – Gender

Please specify your gender.

- Male
- Female

4 – Infrastructure Sector Affiliation

Please indicate the infrastructure sector you are most closely aligned with.

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector

- Defense Industrial Base Sector
- Education Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
- Not affiliated with any of the infrastructures provided above

5 – Technical Hacking Ability

Please indicate whether you have hacking technical skills or no technical hacking skills.

- Hacking skills (hacking ability towards any type of technological hacking, including ethical hackers, penetrations testers, red team/blue team hackers, bug bounty hackers, recreational hackers, education sanctioned hacking, and those affiliated with white hat, gray hat, and black hat hacking, to name a few)
- No technical hacking skills

6 – Education

Please indicate the last education level you completed.

- No schooling or some schooling without a diploma
- High school graduate or equivalent
- Trade/technical training or a college degree
- Master's degree or higher

7 – Employment Sector

Please specify the employment sector you are most closely aligned with.

- Private sector
- Public sector
- Non-Governmental Organization
- Retired
- Unable to work

Using the Likert and Semantic Differential Scales below choose the given options that best align with your position for the research questions.

8 - On a scale from 1 to 5 please indicate how would you rate your

1 – Strongly agree

2 – Somewhat agree

3 - Neither agree nor disagree

4 – Disagree

5 – Strongly disagree

9 - On a scale from 1 to 5 please indicate how you would rate your attitude towards the need for the penalties of criminal hacking to be addressed under one international law?

1 – Strongly agree

2 – Somewhat agree

3 - Neither agree nor disagree

4 – Disagree

5 – Strongly disagree

10 - On a scale from 1 to 5 please indicate how you would rate your inclination on the extent that criminal hacking should be penalized, given it would be implemented globally? See the United States Computer Fraud and Abuse Act (CFAA) penalties chart below, serving as an example for the question.

1 – No penalties

2 – Minimal to less than moderate penalties

3 – Moderate penalties - neither the least of penalties nor the harshest of penalties

4 – More than moderate penalties

5 – Harshest of penalties

Summary of the United States Computer Fraud and Abuse Act (CFAA) Penalties

Offense	**Section in CFAA**	**Sentence***
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.
Source: Prosecuting Computer Crimes Manual, p. 3, CCIPS Division of the DOJ