# HACKTIVISM AND LAW ENFORCEMENT: A QUALITATIVE DELPHI STUDY ON UNITED STATES LAW ENFORCEMENT TECHNOLOGY DEPENDENCY, HACKTIVIST CYBER-ATTACKS, AND AGENCY DEFENSIVE TACTICS

by

Patrick J. Woods

KIMBERLY LOWREY, Ph.D., Faculty Mentor and Chair

MILTON KABIA, Ph.D., Committee Member

OLUDOTUN ONI, Ph.D., Committee Member

Rhonda Capron, Ed.D., Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

September 2018

## Abstract

This qualitative Delphi study examined the perspectives of law enforcement technology experts to build consensus and develop a proactive model for law enforcement agency cyber defense in the United States. The study is responsive to the growing dependency on technology by police agencies, combined with the potential disruption of a hacktivist attack that creates a significant business technology problem. Ten experts assembled for this study hold leadership positions in a state or local law enforcement agency with a combination of 42 years of higher education and 171 years of experience in the law enforcement field, with 143 years dedicated to law enforcement technology management. Experts were interviewed in multiple iterative rounds until consensus and data saturation were achieved. Experts reached consensus on four themes: actively manage messaging and public perception during controversial law enforcement incidents; focus security efforts on critical or sensitive public-facing systems first; increase the rate of successful prosecution of cybercriminals as a preemptive deterrent; and invest in time, money, skills, people, and processes for cybersecurity. From these themes, the Control, Organize, Pursue and Staff (COPS) model for proactive cybersecurity defense was developed. The COPS model focuses on four simple, yet holistic, strategies outlined in the model's acronym: Control the message; Organize systems according to their classifications; Pursue resources, policies and legal avenues to increase the likelihood of arrest and prosecution of cybercriminals; and Staff cybersecurity with the personnel, budget, training and refined processes necessary to mount a formidable cyber-defensive capability.

# Dedication

This research is dedicated first and foremost to the two most important women in my life, my mother and my wife. Each has played an essential role in my success and the completion of this critical component of my educational pursuit. My mother, Dana Phelps, provides unwavering support and led the way, completing her degree while juggling the challenges of being a single mother, working hard to provide for her family. My wife, Leslie Woods, provides the unconditional love and support needed to reach our goals. Her own success and pursuit of higher education have provided the inspiration I needed to keep going, even when motivation was at its lowest. I also dedicate this work to the rest of my family, living and passed. My sister, father, grandparents, and great-grandparents have had a profound effect on my life, ethics, morals, dedication, and zeal for life. Without these qualities, I would not be the man I am today, and this academic achievement would not be possible. Finally, I would like to dedicate this work to my friends, notably Hannah, Ryan, and Abel Hurr, whose friendship and support cannot be measured in value.

## Acknowledgments

I would like to acknowledge my mentor, Dr. Kimberly Lowrey, for her encouragement, support, and availability through this tough, but rewarding, journey. My other committee members, Drs. Oni and Kabia, provided valuable input, and Dr. Tiffany Yates offered her encouragement and energy from day one of this program. I would also like to acknowledge all those who supported me in this journey from the Missouri State Highway Patrol: in particular, Majors Timothy McGrail, ret., and Sarah Eberhard; Captains Larry Plunkett and Christopher Jolly; and Asst. Director Tim Schlueter, each of whom has provided constant encouragement and support to pursue my personal development goals and without whom this journey would be much more difficult.

## Table of Contents

## List of Tables

## List of Figures

# CHAPTER 1. INTRODUCTION

## Introduction

Law enforcement in the United States has been extremely aggressive in the adoption of technologies to modernize department operations, increase efficiency, and improve officer safety (Byrne & Marx, 2011). As law enforcement agencies implement new technologies, police are quickly becoming critically dependent on technology when responding to day-to-day incidents (Sutliff & Richardson, 2016). Nowhere is the dependency more critical than in response to natural or man-made disasters including events of civil unrest (Sutliff & Richardson, 2016). Posing a direct challenge to law enforcement dependency on technology are hackers who, since 2010, have played an increasing role in protests against the government and major corporations through hacktivism, or hacking on behalf of an activist cause. (Coleman, 2014).

Hacktivism describes the actions of hackers inspired by the causes of traditional civil disobedience and driven by social actions. (McCormick, 2013). Hacktivist actions can range from web defacement, a digital form of tagging or graffiti aimed at creatively spreading a sociopolitical message, to distributed denial of service (DDoS) attacks intended to take an entire system or web-based resource offline (Coleman, 2014). Since many government agencies lack the knowledge and preparation to defend against,a government website or system taken offline by a DDoS attack holds the same symbolism as burning a government-owned vehicle in the middle of the street in an effort to shift the arch of control and power (Sauter, 2014b). Without a comprehensive understanding of the technologies employed and proper preparation for advanced cyber threats, law enforcement cannot maintain order successfully on the front lines of the 21st century (Sutliff & Richardson, 2016). Chapter One explains both the background and the problem and identifies the research purpose and question, assumptions, limitations, and definitions. Chapter One concludes with a discussion of the theoretical concepts behind the research.

## Background

Since the late 2000s, law enforcement has increasingly become the target of hacktivists due to traditional physical acts of civil disobedience or other perceived injustices and the media coverage that followed (Sutliff & Richardson, 2016). For example, hackers have aided protests in both the Occupy Wall Street movement of 2010 in New York (Johnson, 2011) and police brutality protests in Ferguson, Missouri, in 2014 (Rogers, 2014). Hacktivist attacks are a significant challenge for police due to law enforcement's increasing use of and dependence upon mobile devices and other technologies (Sutliff & Richardson, 2016). Dependency on technology and a gap in the existing body of knowledge on how to defend law enforcement systems against attacks introduce a new business and operational problem in which agencies responding to incidents of civil unrest or protests are impacted in both physical and virtual operations (World Economic Forum, 2014).

Parallel to the technological evolution of civil disobedience, law enforcement has also gone through several phases of development, adopting new technologies at each stage to aid in responding more efficiently and safely to incidents involving civil unrest (Byrne & Marx, 2011; Newcombe, 2014). For example, a 2015 report from George Mason University identified five categories of technology that were "particularly central to everyday police work and successful practices" (Koper, Lum, Willis, Woods, & Hibdon, 2015, p. 33). The technologies identified by Koper et al. (2015) were technologies for sharing data and crime analysis tools as well as communications, surveillance, and identification technologies. As information technology improves, the response is often an increased dependency on technology creating an increasingly broad and vulnerable attack surface that many law enforcement agencies are underprepared to protect (PERF, 2012).

The targeting of law enforcement systems brought about by police intervention in politically charged incidents is the natural evolution of civil disobedience. However, when combined with a law enforcement agency's growing dependency on technology, these efforts create a significant technological business problem (Bergal, 2017). For example, Lum, Koper, and Willis (2016) found that following the adoption of specific technologies aimed at improving officer awareness and efficiency, many officers lacked the ability to navigate to the location of incidents without the aid of global positioning systems (GPS) or communicate critical incident details efficiently following the degradation of radio or internet service.

The key to understanding the business problem created by the disruption of critical law enforcement technologies by hacktivists is an understanding of the role of police intervention and the associated media portrayal in determining both the likelihood and severity of a cyber-attack against law enforcement agencies (Bergal, 2017; Bonilla & Rosa, 2015; Federal Bureau of Investigation, 2015). For example, Chenoweth and Stephan (2011) found that non-violent protests tend to be more successful than those that rely on violence because of the difficulty in the government's restoration of order against a force portrayed as non-violent.

How law enforcement views and responds to hacktivism and other forms of electronic civil disobedience, as either violent or non-violent, is a fundamental component of understanding the reaction of hacktivists, activists, and the general public and how successful hacktivism will be in the future (Coleman, 2014). The emerging nature of the disruptive threat posed by hacktivists combined with the relative unfamiliarity of the threat and growing dependency on modern technologies by police agencies and society as a whole has created a growing risk (Bergal, 2017; Amoroso, 2016; Chan, 2001; Lum, Koper, & Willis, 2016). The failure to address such a gap places millions of American citizens and visitors at risk, due to possible disruptions of critical emergency services and ultimately, even potential loss of human life. The following section describes the problem statement.

## Business Technical Problem

As technology has evolved into an agent of change in society, technology has also impacted how state and local law enforcement agencies respond to criminal acts and incidents of civil unrest (Newcombe, 2014). According to the technology policy framework developed by the International Association of Chiefs of Police (2014), emerging technologies are critical tools in police work that have the potential to improve safety while making officers more informed and efficient in their daily work.

With the adoption of any technology crucial for daily success, the impact of losing access can have devastating effects on users who depend on the technology (Christensen, Caelli, Duncan, & Georgiades, 2010; Sutliff & Richardson, 2016). One cause of losing access to technology is a cyber-attack targeted at denying service to law enforcement when responding to incidents of civil unrest, commonly tied to hacktivism (Bergal, 2017). Hacktivism is a compound term used to describe hackers with an activist motivation (Infosec Institute, 2013) and defined as a “combination of grassroots political protest with computer hacking” through the “nonviolent use of illegal or legally ambiguous digital tools [to pursue] political ends” (Li, 2013, p. 305). For example, police agencies and officers represent the most visible element of government response to politically charged incidents of civil unrest in the United States and as a result, frequently become the target of hacktivist actions (Wood, 2015). In 2015, the FBI's Internet Crimes

Complaint Center published a public service announcement that warned law enforcement personnel about the threats associated with hacktivists who target law enforcement officials (FBI, 2015).

While numerous recent studies and publications have focused on a wide variety of cybersecurity topics as well as how, what, and why technologies are implemented within law enforcement agencies, limited research has been conducted on how law enforcement agencies address the risks associated with the implementation of police technology (Brooks, 2014; Dodge, 2016; Wood, 2018). The problems presented by the lack of research regarding law enforcement cyber defense is further complicated by the global increase of cyber-attacks across all industries. For example, cyber-attacks have doubled over five years, rising from 68 attacks per organization globally in 2012 to 130 per organization in 2017 (Ponemon Institute, 2017). However, the issue is compounded in law enforcement due to police executives viewing the problem as merely a *computer problem*, failing to recognize the vital role and immense responsibility the executives face in light of the growing threat (Amoroso, 2016).

Law enforcement technology leaders in the United States are presented with the same challenges faced by other information technology (IT) leaders on a daily basis. However, they have the added concern that a technological failure could cause the loss of life for a citizen in need or a co-worker in the line of duty. Due to the often-controversial nature of the work performed by police agencies, there is an increased likelihood that hacktivists targeted law enforcement agencies may interrupt critical public safety applications and infrastructure. Therefore, law enforcement agencies face unique risk and threat mitigation challenges when compared to other industries (Christensen, Caelli, Duncan, & Georgiades, 2010; Sutliff & Richardson, 2016).

The general problem is that the combination of law enforcement's growing dependency on technology and the increasing threat posed by hacktivism has created a potential crisis leaving state and local law enforcement response capabilities vulnerable (Bergal, 2017; Amoroso, 2016; Lum, Koper, & Willis, 2016). Since 2010, events of civil disobedience have escalated changing the severity of hacktivism and the ability to disrupt technologies critical to state and local law enforcement operations (Coleman, 2014). The specific problem is that the effectiveness of hacktivists and the growing dependency on technology by state and local law enforcement has created a more significant attack surface that police agencies are increasingly unprepared to protect (Newcome, 2015).

### Research Purpose

The purpose of this qualitative Delphi study was to develop a proactive defensive model by examining the perceptions and experiences law enforcement technology experts in the United States to identify consensus around the primary influencing factors on the hacktivist targeting of law enforcement agencies and the effectiveness of defensive tactics used by law enforcement agencies in mitigating the impact of hacktivist cyber-attacks.

The problem of increased hacktivist effectiveness and law enforcement's growing dependency on technology affects the lives and public safety of nearly everyone living in or visiting the United States. According to the United States Bureau of Justice Statistics (BJS) (2011), in 2008 there were nearly 18,000 active state and local law enforcement agencies operating in the United States. Police agencies, representing a total force of over 1.1 million personnel, provide law enforcement and investigative services to communities large and small across the United States.

Sutliff and Richardson (2016) of the National Consortium for Advanced Policing found that the threat of a successful cyber-attack is a threat that state and local law enforcement are unprepared to answer. The lack of knowledge and preparedness on the part of law enforcement agencies in the United States underlines the importance of this study, both to build consensus and a working model where one does not currently exist and to protect law enforcement technology against hacktivist cyber-attacks. Without specific actions to improve people, practices, and technology surrounding law enforcement cybersecurity preparedness, law enforcement dependency on technological innovations will make agencies more vulnerable to cyber-attack (Amoroso, 2016). Failure to secure agencies that are critical to the safety and security of our communities leaves every American citizen vulnerable to a hacktivist attack causing loss of services, delay in response, or complete disruption of communication in a time of need.

Current research only indicates the existence and motivation of hacktivism and that law enforcement will likely be a target of hacktivists, either directly or as collateral damage, but provides no solution for the problem (Amoroso, 2016; Bergal, 2017; FBI, 2015). Additional research supports a growing dependency on the same law enforcement technology likely to be in the crosshairs of a hacktivist during a period of civil unrest. However, the existing literature lacks the level of specificity necessary to identify specific systems and defensive techniques that may mitigate such a risk (Byrne & Marx, 2011; Chan, 2001; Lum, Koper, & Willis, 2016). The previous research methods do not account for the consensus of experts who have faced problems associated with the protection of law enforcement technology, worked to overcome challenges, and can contribute to a model aimed at solving the specific problem, which is the focus of this research. Such a model may be implemented by U.S., state, and local law enforcement agencies to protect their agency's critical IT infrastructure. This study will not only advance the research on critical infrastructure protection for the U.S. but also provide actionable steps to be implemented by law enforcement agencies to protect from the adverse effects of a hacktivist cyber-attack.

## Research Question

This qualitative Delphi study examined the perceptions and experiences of law enforcement technology experts in the United States to identify consensus around the primary influencing factors on the hacktivist targeting of law enforcement agencies and the effectiveness of defensive tactics in mitigating the impact of hacktivist cyber-attacks on agency operations. The following is the research question for this study:

> RQ: What better model of cyber security defensive tactics could be developed to prepare U.S., state, and local law enforcement agencies to defend against hacktivist cyber-attacks in the future, as perceived by United States state, and local law enforcement technology experts?

## Rationale

Hacktivism often represents both a valid form of civil disobedience and a potentially destructive force to law enforcement agencies and officers alike (Sauer, 2014; Sutliff & Richardson, 2016). The creation of a model that both respects the importance of online civil disobedience in a modern society and prepares agencies to ensure hacktivism does not adversely affect public or officer safety is critical for state and local law enforcement agencies responding to incidents of civil disobedience.

For the first time in the history of the report, the 2018 Global Risks Report published by the World Economic Forum listed cyber-attacks in the top-three global risks most likely to occur (World Economic Forum, 2018). The annual report, which describes top risks currently facing the world's population as ranked by the World Economic Forum (2018), places the likelihood of cyber-attack third following extreme weather events and natural disasters, respectively. Overall, the World Economic Forum (2018) cites an increasing global dependency on technology and the risk of a critical information infrastructure breakdown as significant trends contributing to the increased focus on dangers associated with a successful attack (World Economic Forum, 2018). In the United States, state and local law enforcement agencies maintain a significant portion of the critical information infrastructure in the form of 911 emergency communications services. Consequently, the disruption of law enforcement technology could have real-world impacts consistent with the World Economic Forum (2018) report (Amoroso, 2016; Greenguard, Mullich, & Parch, 2016; Lum, Koper, & Willis, 2016).

The outcome of the research conducted in this study addresses the critical nature of law enforcement technology and expands upon each of the theories examined in the next section describing the theoretical framework of the study. The next section relates the theories to electronic civil disobedience: most notably, hacktivism. The literature review and the research conducted in this study contribute to a better understanding of how the disruption of critical law enforcement technology caused by hacktivism may impact police operations and what steps are most prudent when developing a police agency cybersecurity strategy.

## Theoretical Framework

The dominant theory for this research is outlined in a working paper from Harvard University's John M. Olin Center for Law, Economics, and Business, titled "A Theory of Civil Disobedience" (Glaser & Sunstein, 2016). Glaser and Sunstein (2016) present a model suggesting that, since civil disobedience is about *signaling* protesters. Activist leaders must determine if a protest will take a patient or *epsilon* approach or whether they will work to achieve *a sweet spot protest* to maximize the impact. The *sweet spot* is described as a protest in which a balance is achieved to ensure enough disruption is caused to draw attention, but not enough to draw universal opposition (Glaser & Sunstein, 2016). Striking the appropriate balance and gaining attention but not opposition, is equally critical to success on the part of protesters as an essential component of determining the strength of law enforcement response and as a significant determinant in the type of defensive actions taken in both in the physical world and cyberspace (Glaser & Sunstein, 2016).

The motivation of hacktivists and the prevailing theory requires the examination of an additional theory to determine the appropriate application of preventative measures. Deterrence theory and its relationship to cyber-attacks, due to the integrated nature of hacking and criminal activity in the physical domain, is particularly well suited for building defenses against cases of hacktivism (Goodman, 2010). Deterrence theory is outlined broadly in a variety of academic works, but most recently in work published in 2004, detailing its application in modern culture and sociopolitical issues (Freedman, 2004). At the core of the deterrence theory is the deterrent declaration that in reaction to action or lack of action, a particular outcome will occur sometimes in the form of deterrence through denial (Freedman, 2004). Denial in electronic disobedience cases can be achieved through a reduction in capability, communication, and credibility (Goodman, 2010).

The argument for applying deterrence theory to cyber-attacks is that it provides a fundamental framework on which cybersecurity preventative measures may be built (Geers, 2010). For example, a reduction in capability may be accomplished through increased defenses and capacity, reducing the ability of the attacker to successfully launch DDoS attacks, a common tactic among hacktivist actors (Coleman, 2014). A denial in communication may be aided by increased cooperation among international law enforcement agencies in pursuing cyber actors, which also aids in the third element of credibility by reinforcing the potential consequences of taking part in criminal hacktivist activities (Geers, 2010).

To succeed in the application of deterrence theory to hacktivism through a reduction in capability or denial of communication requires the examination of the theory behind activist actions, called the social movement theory (Kurzman, 2003). Similar to deterrence theory, social movement theory is outlined broadly in a number of academic works that describe its application to both national and international social protests and activist movements, each attempting to explain how and why movements develop in the first place (Kurzman, 2003).

In attempting to explain the mobilization of hackers and the alignment of the actions of hackers with social causes, Sonderberg (2013) developed the concept of collective action, which describes how broader social movements form around an interpretation of the world that adds purpose to the group (digitally organized or physical) and unites the group around a common struggle. Unlike an ideology, where loyalties and commitment run much deeper, collective action framing is more fluid and susceptible to disruption through an effective defense focused on counter-information campaigns (Soderberg, 2013).

While "social movement theory is an obvious choice to explain political mobilization online" (Beyer, 2014, p. 142), there is a gap in the literature regarding the application of the theory to internet-based activism. As Beyer (2014) explained, most research, as it relates to the application of social movement theory to online activism, has been conducted by trying to compare online activist activity to traditional offline behaviors. This allows for additional research on how online social movements impact and even encourage the growth of physical protests, both of which impact law enforcement activities. The online mobilization of protesters has resulted in activism that has spread globally and allows many more people to participate unified in a common purpose with the potential of widespread disruption if left uncontrolled. Prior to the introduction of social-media and technology, activism was usually contained locally and limited in the number of participants motivated through traditional media to participate (Beyer, 2014).

## Significance

While numerous recent studies and publications have focused on a wide variety of cybersecurity topics as well as how, what, and why technologies are implemented within law enforcement agencies, very little research has been conducted regarding how law enforcement agencies address the risks associated with the implementation of police technology (Brooks, 2014; Dodge, 2016; Wood, 2018). The problems presented by the lack of research regarding law enforcement cyber defense are further complicated by the increase of cyber-attacks across all industries globally. For example, cyber-attacks have doubled over five years rising from 68 attacks per organization globally in 2012 to 130 per organization in 2017 (Ponemon Institute, 2017). However, police executives have viewed the problem as merely a *computer problem*, failing to recognize the vital role and immense responsibility the executive faces in light of the growing threat (Amoroso, 2016).

A key factor contributing to a lack of executive engagement in cybersecurity issues is a lack of awareness surrounding complex technological issues and more importantly, the lack of a clear, easy to implement model of cybersecurity defense (Rothrock, Kaplan, & Van Der Oord, 2018). The outcome of this study has the potential to provide a simple, yet effective solution to the nearly 18,000 state and local law enforcement agencies in the U.S. for the development of cyber defense capabilities and a better understanding of the potential threat posed by hacktivism.

Hacktivists share many common characteristics. Traditional hacking techniques are used by both hackers and hacktivists and the two different groups primarily only differ in their motives (Jordan, 2016). Traditional hackers usually have a wide range of motives, including financial gains and the thrill of a challenge (Jordan & Taylor, 1998). Hacker tactics include technical exploits, social engineering, brute-force access attempts, and other approaches to attacks on the confidentiality and integrity of systems (Jordan, 2016). Conversely, hacktivists are primarily motivated by social and activist causes and focus attacks on system availability and a targeted organization's reputation (Jordan, 2016). Tactics of hacktivists include defacements of websites (equivalent to graffiti or other destruction in the physical space), denial of service (equivalent to shutting down roads or blocking access to services), and doxing (collecting and disseminating information, often private, on the principal individuals in an attempt to embarrass, threaten or otherwise coerce a particular person) (Coleman, 2014). Defensive models to protect against attacks from both hackers and hacktivists exist in the form of national and international frameworks, such as the ISO 27000 series and the National Institutes of Standards and Technology (NIST) National Cybersecurity Framework (Moraetes, 2018). Both frameworks comprise security governance, technical controls, and other steps organizations can take to protect technology from the adverse effects of an attack (Watson, Tellabi, Sassmannahausen, & Lou, 2017). However, these frameworks fail to address the unique steps law enforcement agencies can take to prevent an attack or deter hacktivists from attacking a police agency, which is the focus of this study.

The current study contributes to the body of research by adding a cybersecurity defensive model designed specifically for law enforcement in the United States. The study fills the gap in research on securing police technologies from the emerging global threats posed by cyber-attacks. The research addressed the specific types of attacks most likely to be encountered by law enforcement agencies during times of organizational crisis while providing executives an actionable model on which to build a formidable defensive posture in every law enforcement agency across the country.

## Definition of Terms

*Attack Surface:* Attack surface is defined as a set of methods, vulnerabilities, and exposures to which a system is vulnerable to attack and potential damage (Manadhata & Wing, 2010).

*Civil Disobedience*: Civil disobedience is an often non-violent, legally ambiguous, and conscious public action taken by individuals or groups with the goal of bringing about socioeconomic or sociopolitical change (Stanford University, 2013).

*Civil Unrest:* Civil unrest is a state during and immediately following incidents involving group actions, both violent and non-violent, that are disruptive to the ordinary course of civic or economic activity (Ramakrishnan et al., 2014)

*Criminal Act:* A criminal act is defined as the process of violating a law or legal requirement (Andrews & Bonta, 2014)

*Deterrence:* Deterrence is the act of influencing the actions of another, particularly to guide the other person away from one action or outcome toward another outcome more desirable to the influencing party (Freedman, 2004)

*Distributed Denial of Service (DDoS)*: A DDoS attack is a form of cyber-attack delivered with the intent of interrupting access to a computer system, application, or network by various means, including flooding the system with malicious or false traffic from multiple disparate sources (McDowell, 2013).

*Electronic Civil Disobedience:* Electronic civil disobedience is a hybrid form of non-violent and legally ambivalent actions utilizing technology as a means to bring about socioeconomic or sociopolitical change (Wray, 1999).

*Emerging Technology:* Emerging technology is defined as a process, product or evolution that is still in a phase of development or early adoption (Stevens-Henager College, 2013).

*Hacktivism*: Hacktivism is the act of using computer hacking techniques to engage in civil disobedience or other actions aimed at advancing a political, economic or social ideology or change (Stanford University, 2016).

*Hacktivist*: A hacktivist is a person engaged in the act of hacktivism, usually motivated by a desire to influence political, economic or social policy (Stanford University, 2016).

*Internet Protocol:* Internet protocol (IP) is an open source standard for communication between computing devices across a diverse network infrastructure. IP has become the most widely used standard for communication across the internet and local area networks (Deering & Hinden, 2017)

*Law Enforcement*: Law enforcement is a discipline and profession in which agencies and agents of the government carry out acts to maintain law and public order through the uniform enforcement of applicable laws (U.S. Department of Justice, 2016).

*Web Defacement:* Web defacement is an action in which a hacker or other actor makes unauthorized changes to a public website as a means to embarrass the targeted organization or spread a political or social message (Workman, Phelps, & Gathegi, 2012).

## Assumptions and Limitations

### Assumptions

The first assumption of this research study was that the experts making up the panel possessed an essential awareness of hacktivism and recent national events involving law enforcement actions that sparked events of civil disobedience. The second assumption was that experts were truthful and forthcoming with their answers and unencumbered by local policies and politics. The third assumption is that some pattern exists within hacktivist actions against the police that can be drawn upon to guide questions to experts on this topic.

### Limitations

The first limitation is that, while law enforcement executives are typically well attuned to domestic affairs involving their profession, the cyber-attack elements of incidents of civil disobedience are likely overshadowed by physical protests and demonstrations widely disseminated in the media. Government technology experts frequently perform work for multiple agencies and may not be as attuned to specific threats that face the law enforcement agencies served. The second limitation is that the underlying events in the vast majority of hacktivist actions where law enforcement is involved are often high-profile and politically charged, which may limit participation by otherwise knowledgeable experts. Local policies may restrict specific information regarding defensive measures and tactics that may reveal key system vulnerabilities.

The third limitation is that hacktivism's sporadic, disorganized nature is unpredictable, and may present an issue with developing a pattern over an extensive period. An additional general limitation is that the phenomenon of hacktivism is still in its relative infancy. Scholarly research and grounded theories in the area, specifically as related to law enforcement, is limited. The fourth limitation is that the Delphi method is dependent on the opinions of the experts selected to participate in the study and the results are only as good as the quality of the responses provided by the experts. The fifth limitation is that this researcher has extensive experience in the field of law enforcement technology and cybersecurity, which could introduce bias into the study. Bias will be controlled by avoiding experts from the same geographic area (state) as the researcher to avoid the researcher and a participant sharing common experiences tied to a particular event.

## Organization of the Remainder of the Study

Chapter One explained the problem that the effectiveness of hacktivists and state and local law enforcement's growing dependency on technology have created a more significant attack surface that police agencies are increasingly unprepared to protect, as well as, the purpose, research design, rationale, theoretical orientation, and significance of this study. Chapter Two examines the available literature on the topics surrounding hacktivism and law enforcement technology as well as analysis and syntheses of this literature to support the overall purpose of this study. Chapter Three details the research methodology and overall design for the current study, including plans for addressing bias and any lingering issues of validity in the study.

Chapter Four provides a detailed account of the data collection and analysis conducted by the researcher. In Chapter Five, the results and findings of the data collection and analysis are presented, including a discussion regarding the impact and recommendations of the study's conclusion. Additionally, the researcher will present a model for law enforcement agency cyber defense based on the study findings.

# CHAPTER 2. LITERATURE REVIEW

## Introduction

Chapter Two provides an exhaustive review of literature related to the problem statement on the effectiveness of hacktivist actions and the growing dependency on technology by state and local law enforcement, which creates a significant attack surface that police agencies are increasingly unprepared to protect. Chapter Two is divided into five sections. Chapter Two includes an explanation of the methods used to search the literature, a literature review, a synthesis of the research findings, and a critique of the previous research methods.

## Methods of Searching Literature

Literature for Chapter Two was searched using a mixture of peer-reviewed and trade articles from Google, Google Scholar, and database searches within the Capella University Library. Particular attention was placed on ensuring non-scholarly industry journals and government documents were both reputable and relevant. The information presented represents the synthesis of research data collected from over 100 sources, representing a mixture of scholarly peer-reviewed journals, trade journals, government documents, dictionaries, research books, and technical documentation.

## Review of the Literature

### Civil Disobedience in the United States

The United States of America was founded on principles of individual freedom and liberty (Friedman, 2005). One of the cornerstones of the right to individual freedom and liberty is the ability to speak and protest peacefully when a citizen feels they are experiencing injustice (Friedman, 2005). The Declaration of Independence guarantees Americans the right to "life, liberty and the pursuit of happiness" (United States, 1776) and the Bill of Rights guarantees liberty through the First Amendment by prohibiting the government from “abridging the freedom of speech, or of the press; or the right of the people to peaceably to assemble” (United States Const. amend. I).

Because of the liberty granted to United States citizens through the Constitution, the United States has experienced periods of uprising and protest since the founding of the nation (Tilly & Wood, 2015). Over time, the methods for expressing displeasure with the government have evolved and been counteracted in different ways (Andrews & Gaby, 2015; Beyer, 2014). From the revolution that led to the founding of the United States as an independent nation to the digital protests of today, the United States has witnessed both violent and non-violent means to the same desired end: political or social change (Beyer, 2014).

A mid-19th-century essay by Henry David Thoreau introduced the term *civil disobedience* and a new way of exercising protest rights in the United States (Sauter, 2014b). In the essay, Thoreau (1849) presented a case for citizens to stand up against government overreach peacefully, even at the risk of going to jail: “Under a Government which imprisons any unjustly, the true place for a just man is also a prison” (p.2). Through the decades that followed, American history has been filled with examples of demonstrations for a variety of reasons (Andrews & Gaby, 2015). Some demonstrations remained peaceful, while others were pushed to violence by one side or the other (Andrews & Gaby, 2015). Although the causes and protesters often change, the common element in each instance is the police, who represent the government in the restoration of order (Smith, W., 2016).

Dr. Martin Luther King, Jr., echoed Thoreau’s belief that successful civil disobedience requires a reaction from the police. Dr. King, Jr., the leader of the modern civil rights movement, explained that resistance to police action is nearly essential in effecting change through civil unrest in his 1963 *Letter from Birmingham jail* (King, 1963).

In the letter, King (1963) wrote:

> I submit that an individual who breaks a law that conscience tells him is unjust, and who willingly accepts the penalty of imprisonment to arouse the conscience of the community over its unjustice is in reality expressing the highest respect for the law (p. 7).

Although neither Thoreau nor King called directly for targeting police in response to, or in retribution for, their arrests, both argued that some form of disruption and interaction with police, acting as government officials, is key to the very idea of civil disobedience (Siff, 2016).

As the idea of civil disobedience began to take hold over the course of United States history, organizers began to refine efforts to humanize the civil disobedience movements, a factor that still contributes substantially to the spread and effectiveness of a civil disobedience campaign, particularly with the modern introduction of social media (Wanzo, 2015). For example, years before Rosa Parks made her famous stand on the bus in Montgomery, Alabama, in 1955, two other women had made a similar stand and were arrested in March and October. However, these ladies were determined to be too undesirable to be the face of a movement (Wanzo, 2015). The idea of humanizing civil disobedience movements, such as selecting Rosa Parks based on personal characteristics, continues to serve as a critical ingredient in the rapid spread of civil disobedience movements that appeal to the emotional aspects of victims, particularly as it relates to the hacktivist response to police intervention (Mikhaylova, 2014). The desire for movements and participants to strike the right balance and the appropriate use of civil disobedience led to the development of the theory of civil disobedience (Glaser & Sunstein, 2016).

## Theory of Civil Disobedience

The emergence and development of civil disobedience developed into a theory of the *sweet spot* for disobedience (Glaser & Sunstein, 2016). Outlined in a working paper developed at Harvard University, titled *A Theory of Civil Disobedience* (Glaser & Sunstein, 2016), the authors propose a theory that suggests civil disobedience is about *signaling* protesters and to optimize effectiveness, organizers must take a mild or *epsilon* approach through what is called *a sweet spot protest* (Glaser & Sunstein, 2016). The *sweet spot* is described as a protest in which a balance is achieved to ensure enough disruption is caused to draw attention, but not enough to draw universal opposition (Glaser & Sunstein, 2016).

Glaser and Sunstein (2016) attempted to examine civil disobedience by organizing incidents of disobedience based on the productive power of the group to reach a more in-depth understanding about the decision to engage in such an act. Glaser and Sunstein (2016) proposed that three primary categories of civil disobedience based on the effective power of the protesting group. The first category of civil disobedience is revolution. Revolution is based on the assumption that the protesting group possesses enough power and influence to overcome the power of the government the group opposes (Glaser & Sunstein, 2016). Ensured bargaining, representing the second category of civil disobedience, is on the opposite end of the spectrum, relating to groups that are either too weak or have only a minimal appetite for even the mere possibility of violence (Glaser & Sunstein, 2016). Revolution may be very relevant to police agencies outside of the United States in developing countries, whereas ensured bargaining is of particular relevance to the private sector in the context of a labor dispute where hacktivist actors may become involved in support of the labor movement (World Economic Forum, 2014).

The third category of civil disobedience, according to Glaser and Sunstein (2016), includes actions with the intent to provoke authority and shift public perception. Although all three categories of acts of civil disobedience are possible within the United States, only the acts of provoking authority and shifting public perception are particularly relevant as they relate to the examination of law enforcement being targeted by hacktivists. For this study, the focus is on the third category, in which groups engaging in civil disobedience or protest are likely motivated to attempt to provoke authority and shift public opinion in the process (Glaser & Sunstein, 2016).

Glaser and Sunstein (2016) suggest that groups that are too weak to generate a revolution or cause significant harm to political leadership will instead aim to drive change through the lens of perception, either by provoking a hostile government response or the silence of no response. Glaser and Sunstein (2016) provide the examples of two events where the protesting groups faced off with police in a very public way: Ferguson, Missouri in 2014 and Baltimore, Maryland in 2015 (Glaser & Sunstein, 2016). For example, in both Ferguson and Baltimore, protesters took to the streets following incidents of perceived excessive use of force by the police against young African-American men (Glaser & Sunstein, 2016). According to Glaser and Sunstein (2016), the protesters used the short-term objective of indicting the officers involved in the incident and the long-term objective of changing law enforcement's treatment of minorities, particularly African-Americans, to establish goals in order to galvanize others to join in or *signaled* other protestors. In both instances, the *signaling, or* establishing and communicating of common goals worked and drew protesters both to the streets and online to participate in acts civil disobedience and some goals were achieved in the process (Glaser & Sunstein, 2016). Violence also played a crucial role in determining the public perception of the action. Violence and destruction of property by the protesters resulted in media coverage and public perception that did not foster the universal support necessary to ensure the desired outcome of the movement. These acts of civil disobedience missed the mark of a *sweet spot* protest (Glaser & Sunstein, 2016).

The overall success or failure of a civil disobedience movement, primarily driven by adequately managed publicity and non-violence as a critical determinant, was the subject of a 1971 book by American political philosopher John Rawls (Rawls, 1971). Rawls (1971) suggested that, much like Glaser and Sunstein's concept of *signaling*, in order to be considered an act of civil disobedience, the act must be completed in public with sufficient communication to authorities regarding the purpose of the act. Rawls (1971) contended that once a disobedient act becomes destructive or violent, or interferes with the civil liberties of others, the message and purpose behind the action become obscured and are less likely to achieve universal support.

Striking the appropriate balance and gaining attention but not opposition are equally critical to protesters' success, but are also an essential component in determining the strength of law enforcement response and a significant determinant in defensive actions taken in both the physical world and cyberspace (Glaser & Sunstein, 2016). What Rawls could not have foreseen in 1971 is the availability and velocity of communication introduced by the advent of social media which allows protesters to broadcast to the authorities and others around the world, increasing support for the movement from around the globe (Cammaerts, 2015). The following section consists of a comparison of different hacker groups, their motivation, and their tactics.

## Comparing Hacker Groups by Motivation and Tactics

In a 2016 peer-reviewed article, Jordan (2016) sought to summarize the history of hacking, an ambiguous term formulated from multiple different perspectives. Jordan (2016) presented evidence to support four phases within the *genealogy* of hacking: prehistory, the golden age of cracking, hacking divided, and a state of full consciousness of state-sponsored attacks. Each phase represents a distinct evolution in the methods and motives behind the hacker culture (Jordan, 2016). One new phase is called *cracking. Cracking* refers to attempting to illegally break into computer systems through a number of both technical and non-technical techniques (Jordan, 2016). The golden age of cracking is the era where hacking took a distinct turn from those who were often hobbyists in search of the thrill associated with exploiting loopholes in technology as a sort of sport (Jordan, 2016). The crackers of the golden age represent the genesis of the six broad categories of modern hackers, as determined by their tactics and motivations.

According to a 2018 report by the White House and The Council of Economic Advisors, the U.S. government recognizes six broad categories of malicious *cyber threat actors*: nation-states, corporate competitors, organized crime groups, opportunists, company insiders, and hacktivists (United States Council of Economic Advisors, 2018). Nation-states, corporate competitors, and organized crime groups share many of the same general motivations and tactics because they are generally motivated by leverage or financial gain and utilize tactics focused primarily on confidentiality attacks against private data and intellectual property (United States Council of Economic Advisors, 2018). Where these groups differ is in the scope and scale of such attacks. Whereas nation-states may focus on a wide range of targets, from an entire rival country to spying on a single individual, corporate competitors are primarily focused on their industry competitors, and organized crime groups are focused on any person or organization likely to earn the group's most significant financial gain (Bejtlich, 2015).

The remaining three groups each maintain their own unique sets of motivations and tactics, which is significantly more challenging to predict. Company insiders, typically employees who are either disgruntled or recently separated from a company, can be motivated by external factors that include a grievance with the company, financial hardship, loyalties to competitors, or even extortion (Dalal & Gorab, 2016). Since insiders typically have access to many applications containing sensitive data, these actors can represent some of the most dangerous if undetected (Dalal & Gorab, 2016). Opportunists are typically motivated like traditional hackers, seeking the notoriety and thrill associated with testing how far they can stretch the limits of technology through the use of a wide variety of hacking tools with the intent of negatively impacting the confidentiality, integrity, and availability of target systems (United States Council of Economic Advisors, 2018). The last group and the most applicable to this study are hacktivists. Unlike all other groups explored through the literature, the motivations of hacktivists are primarily ideological and are viewed as an attempt to correct a social injustice (Sauter, 2013). This often-heterogeneous group does not always represent a single person or sponsoring entity, meaning that their motivations, skill level, and tactics are mostly unpredictable (Sauter, 2013). The following section discusses the emergence of technology-based civil disobedience.

## The Emergence of Technology-Based Civil Disobedience

Since the mid to late 2000s, a new method of civil disobedience was created by the advent of the internet and the emergence of hackers as a cultural force (Mikhaylova, 2014; Sauter, 2013). Hackers created the term *electronic civil disobedience* or, more recently, hacktivism, using skills designed to support breaches or disruptions of computer systems to support an activist cause (Coleman, 2014; McCormick, 2013). The objectives behind hacktivist actions are not that different from traditional civil disobedience: that is, to disrupt, destroy, embarrass or otherwise expose those who are behind the perceived injustices (Beyer, 2014; Bonilla & Rosa, 2015; Sauter, 2013). Tactics, however, are different, since most of the acts take place in the alternate dimension of cyberspace (Sauter, 2013). Hacktivist activities include defacement of websites (equivalent to graffiti or other destruction in the physical space), denial of service (equivalent to shutting down roads or blocking access to services), and doxing (collecting and disseminating information, often private, on the principal individuals in an attempt to embarrass, threaten or otherwise coerce a particular person) (Coleman, 2014). As a reaction to police involvement or in response to emotionally-charged incidents, law enforcement officers are a frequent target of hacktivist actions (Bergal, 2017; FBI, 2015).

The examination of the development and motivation behind hacktivism and, ultimately, its threat to law enforcement, is a two-phased approach. As explained in Chapter one, hacktivism is a compound term defined as the use of computer hacking techniques to engage in civil disobedience or other actions aimed at advancing a political, economic or social ideology or change (Li, 2013). Because of the compound nature of the term, the concept must be explored by looking at activism and, more specifically, it's relation to possible disruption of law enforcement technology, civil disobedience, and incidents of unrest in addition to the history and sociology of hacking.

Jordan (2016) suggests that during the third phase of the genealogy of hacking is known as *hacking divided*. In this phase, hackers still viewing hacking mainly as a hobby remained while another subgroup emerged that was focused on hacking for political causes, known as hacktivists. Jordan (2016) described this new sub-activity as "mass action hacktivism, which attempted to reinvent mass demonstration and civil disobedience tactics in online settings" (p. 10). The increase and spread of the internet and computer software access along with new motivations pushing acts of civil disobedience to the internet enables protests to grow in structure and number making it easier for protestors to launch wide-scale denial of service attacks once the group rallied around a specific cause (Jordan, 2016; Harris, Konikoff, & Petersen, 2013).

To explain the phenomena that occurred during the hacking divided phase, exploring the sociology at work in the hacker culture is required. In an earlier peer-reviewed journal, Jordan and Taylor (1998) found that six major internal factors contribute to the *hacker culture* or, the *hacking community* in which hackers operate. Internal factors include technology, secrecy, anonymity, boundary fluidity, male dominance, and motivations. While each factor can contribute to a hacker latching on to the hacktivist cause, the motivation of being a part of a higher cause or community has the influence (Jordan & Taylor, 1998).

Jordan and Taylor's (1998) research identifies two particular elements of hacker motivation that expose a direct link to the adoption of a political or activist cause. The first is the awareness that the *hacker* label or mystique is often foreign to those outside of the community and can often lead to tighter bonds among the community and positive recognition for expert skills and accomplishments (Jordan & Taylor, 1998). The feeling of camaraderie can manifest itself beyond the hacker community into a desire to feel the same sense of community and recognition among a broader community of activists.

The second motivation, according to Jordan and Taylor (1998), is the ability to gain access to take down systems that are *off limits*, which brings a sense of power and control that some in the hacking community may seek. Launching attacks in the name of a cause only further bolster some elements that motivate the hacktivist group (Jordan & Taylor, 1998). The broader sense of community often forms tight bonds that can quickly help distribute tools, propaganda and target lists, which only further challenges law enforcement agencies when defending against a potentially massive *Distributed Denial of Service* (DDoS) attack (Coleman, 2014). DDoS attacks are aimed at disrupting legitimate online services through an overwhelming amount of network traffic in a coordinated attack from multiple sources aimed at a single target and have become a mainstay of the modern electronic civil disobedience toolkit (Somani et al., 2017).

In a 2013 report from Carnegie Mellon University, researchers noted that the attack techniques aimed at disrupting or damaging legitimate communications systems have been in a constant state of evolution since approximately 1998, the year the first recorded DDoS attack tool was discovered (Harris, Konikoff, & Petersen, 2013). In the case of a cyber-attack, Harris, Konikoff, and Peterson (2013) document three phases of the traditional *cyber-kill-chain*, relevant to a DDoS attack as popularized by defense firm Lockheed Martin: reconnaissance, exploitation, and command and control. Each phase offers police agencies the opportunity to disrupt the attack (Harris, Konikoff, & Petersen, 2013).

The success of the DDoS attack is primarily determined by the appropriate selection of a target, the ability to recruit enough participants or bots to generate sufficient traffic, and the ability to keep the group engaged long enough to have the desired impact. Most DDoS attacks aim to overwhelming target a system by launching non-legitimate requests to connect as a user or creating bandwidth consuming traffic (Harris, Konikoff, & Petersen, 2013).

Contributing to the rapid growth and application of electronic civil disobedience and the success of DDoS attacks is the widespread availability of information and recruitment opportunities made possible through social media platforms and portable electronic devices capable of collecting video, audio and other media real-time (Coleman, 2014). Now hacktivist collectives can recruit participants through social media, where the group can not only work to select targets but also recruit to build a network of cyber disruptors (Harris, Konikoff, & Petersen, 2013). Modern communication methods have bridged the divide between the cyber-attack hacker and activist communities, blending the message and mission of two otherwise heterogeneous groups in modern instances of civil disobedience (Coleman, 2014). For example, in a 2015 article in the *Journal of the American Ethnological Society*, the authors contrast the velocity of the movements following incidents of perceived police brutality between the 1991 case involving Rodney King in Los Angeles, California and the 2014 incident involving Michael Brown in Ferguson, Missouri (Bonilla & Rosa, 2015). While the historical divide between the two events spanned more than twenty years, a common bond beyond the racial tension forever ties the events in Los Angeles and Ferguson together: the way the message spread from a localized event to a global phenomenon (Harris F., 2015; Harris, Konikoff, & Petersen, 2013).

Bonilla and Rosa (2015) cited how the 1991 Rodney King incident gained national attention because of a home-made VHS tape, which was given to the traditional media and created a national outpouring of support over the perceived injustice done to Mr. King. Bonilla and Rose (2015) found that in 2015, nearly 56% of the United States population carried a video-enabled mobile device. This increase in access to recording devices allows for more frequent recording of localized incidents of perceived injustice. Bonilla and Rosa (2015) highlight the role of social media platforms in allowing citizen journalists or activists to globalize an otherwise local incident in a matter of moments, such as what happened with the Ferguson movement on social media in 2014.

Modern citizen-journalism activity highlights a significant aspect of the non-traditional attack role that electronic civil disobedience plays in the earliest phase of a DDoS attack, in which potential attackers are beginning to select targets, known as reconnaissance (Harris, Konikoff, & Petersen, 2013). The velocity, volume, and tone of the information being transmitted to the broader global audience of the hacker communities behind the attacks play a significant role in determining which police agencies are likely to be targeted and the ability for an organization or agency to disrupt the attack in the reconnaissance phase of the cyber-kill-chain (Harris, Konikoff, & Petersen, 2013).

While police agencies can do little in a society focused on civil liberty protections to disrupt the message being broadcasted by the activists and sympathizers, Coleman (2014) found that agencies can have an impact on the message shared through traditional and social media platforms. Police agencies can interrupt, disrupt, or deter hacktivist messaging by engaging with the media and the general public with frequent and transparent messaging. This can have a positive effect and counteract the negative sentiment toward the law enforcement agency during incidents of civil disobedience (Coleman, 2014). The following section summarizes how police respond to civil disobedience, which is a major factor in influencing the success or failure of hacktivist cyber-attacks.

### Police Response to Civil Disobedience Determines Cyber-Attack Results

The emotional and political aspects of incidents involving civil disobedience pose a significant challenge to the police when the incident crosses the threshold into an incident of civil unrest, which mainly occurs when the event includes both violent and non-violent participants. Regardless of the presence of violence, incidents of civil unrest necessitate a response to restore order (Chenoweth & Stephan, 2011). As detailed in the 2011 book *Why Civil*

*Resistance Works: The Strategic Logic of Nonviolent Conflict*, Chenoweth and Stephan (2011) summarized numerous case studies that found non-violent protests present difficulties for the government when trying to restore order, because it is difficult to assert force against a protesting force that appears to be non-violent. Any perceived aggression by the police, as agents of the government, tends to appear heavy-handed and unnecessary when considering limited potential damage or public harm as the alternative (Chenoweth & Stephan, 2011).

Similar to how the theory on civil disobedience calls for protest organizers to be balanced in approach toward combating perceived injustice (Glaser & Sunstein, 2016), police leaders must be balanced in responding to incidents of civil unrest. Police leaders must find the right balance of the application of the use of force and transparency when attempting to restore public order (Chenoweth & Stephan, 2011). Failure to strike such a balance may leave the general public conflicted on which side is standing for a just cause and elicit an undesirable reaction (Glaser & Sunstein, 2016).

Some of the most vividly documented cases of police response to civil unrest that appeared out of balance come from the civil rights movement of the 1960s (Andrews & Gaby, 2015). For example, during the summer of 1963, President John F. Kennedy was so moved to action by the response of southern state police agencies to the growing incidents of civil unrest that he sent federal authorities to seize control of a situation which was quickly spiraling (Andrews & Gaby, 2015).A ten-week stretch in the spring of 1963 saw nearly 13,000 arrests from 758 estimated demonstrations, portrayed in the media as violent clashes between protesters and police and most widely remembered as the police being the primary aggressors (Andrews & Gaby, 2015). According to Glaser and Sunstein (2016), who borrowed a term from the theory of civil disobedience, the protesters and even the federal government had been *signaled* to the movement occurring in the south as a direct result of the police action (Glaser & Sunstein, 2016). While not a technical problem on its own, the ability to control or otherwise disrupt this *signaling* through proactive communication and community engagement may hold the key to preventing a hacktivist cyber-attack from occurring with a tactic known as cyber deterrence (Denning, 2015). The following section examines the feasibility of cyber deterrence.

**The Feasibility of Cyber Deterrence**

Implementing deterrence as a method to keep evil forces in the world at bay dates back to the mid-seventeenth century (Hobbes & Gaskin, 1998). In the literary work *Leviathan*, first published in 1651, the political philosopher Thomas Hobbes described humans as creatures of their own volition who, when left to their own devices, will pursue self-interest as long as the value proposition remains in favor of the one making the decision (Hobbes & Gaskin, 1998). *Leviathan* established the foundation for the theory behind deterrence, a method aimed at dissuading an otherwise bad actor from a detrimental action by changing the value proposition through the threat of harm to the actor's self-interest.

Modern-day deterrence theory developed during the Cold War era, when tensions regarding nuclear war gripped the United States and the U.S.S.R. in a relative stalemate that lasted for decades (Quackenbush & Zagare, 2016). Deterrence theory evolved and is outlined broadly in a variety of academic works, but is found most recently in work published in 2004, which details the application of deterrence theory in modern culture and sociopolitical issues (Freedman, 2004). At the core of the modern deterrence theory is the deterrent declaration, which states that, in reaction to action or lack of action, a particular outcome will sometimes occur in the form of deterrence by denial (Freedman, 2004).

Denial in electronic disobedience cases can be achieved through a reduction in capability, communication, and credibility (Goodman, 2010). For example, a reduction in capability may be accomplished through increased defenses and capacity reducing the ability of the attacker to successfully launch DDoS attacks, a common tactic among hacktivist actors (Coleman, 2014). A denial in communication may be aided by increased cooperation among international law enforcement agencies in pursuing cyber actors, which also supports the third element of credibility by reinforcing the potential consequences of taking part in criminal hacktivist activities (Geers, 2010). Applying deterrence theory to cyber-attacks provides a fundamental framework on which cybersecurity preventative measures may be built (Geers, 2010).

To gain success in the application of deterrence theory to hacktivism through a reduction in capability or denial of communication requires the examination of the theory behind activist actions, namely social movement theory (Kurzman, 2003). Similar to deterrence theory, social movement theory is outlined broadly in a number of academic works detailing its application to both national and international social protests and activist movements. Each theory attempts to explain how and why movements develop in the first place (Kurzman, 2003). In most cases, social movements begin in support of a particular idea or ideology driving like-minded individuals to collective action (Soderberg, 2013).

Soderberg (2013) defined the concept of collective action framing, as the way in which broader social movements form around an interpretation of the world that adds purpose to the group (digitally organized or physical) and unites hackers in a common struggle. This definition helps to explain the mobilization of hackers and the alignment of the hackers' actions with social causes (Soderberg, 2013). Falling short of an ideology, where loyalties and commitment run more deeply, collective action framing is much more fluid and more susceptible to disruption through an effective defense focused on counter-information campaigns, an ideal method for applying deterrence theory in the practice of cybersecurity. (Soderberg, 2013).

While the application of deterrence theory to cybersecurity may seem relatively straightforward in its primary application, the reality of its execution in cyberspace is a bit more complicated (Geers, 2010). The malleability of cyberspace and the ability to operate in relative anonymity disarm some of the most fundamental tenets of determining the effectiveness of criminal deterrence (Denning, 2015). For example, Denning (2015) found the use of anonymizing technology and the cover of international law to be significant barriers to criminal apprehension and deterrence online.

In a seminal piece of literature on criminal deterrence, Kevin Kennedy (1983) cited two primary requisites for effective criminal deterrence. The first requisite is certainty and severity, suggesting that the likelihood of getting caught in the act must be certain and that the severity of the punishment must be enough to change the value proposition of the action (Kennedy, 1983). According to Kennedy (1983), the second requisite of criminal deterrence is credibility and communication. The potential hacker must understand that the threat of being caught comes from a credible source and that this threat is well understood by the potential threat actor (Kennedy, 1983). Even though coordination may be difficult, it is critical that law enforcement agencies and courts work together to enhance the prosecution of hackers not only to punish those responsible but also increase the credibility of the threat of being caught. The application of deterrence to cyber-attacks is challenged by the difficulty in attributing attacks to specific hackers, the ease by which cyber weapons are obtained, the number of hackers engaged in the cyber-attacks, and the ability of the police force to enforce laws across international borders (Denning, 2015). Unlike the application of deterrence theory to nuclear conflict, where all parties broadly understand the likely outcome of retaliation for an attack and the proliferation of offensive and defensive countermeasures are evenly balanced, cyber-based conflict makes the outcome of retaliation (punishment) much less clear (Denning, 2015). For example, the cost of offensive cyber capabilities is minor in comparison to the enormous costs associated with an active defense, which may be a barrier to law enforcement agencies gaining the full effect of deterrence (Freedman, 2004; Denning, 2015).

The National Institutes of Justice released a publication on general deterrence in 2016 titled “Five Things About Deterrence,” that offers some essential guidance for ideas applicable to deterrence in both physical and cybercrimes (National Institute of Justice [NIJ], 2016). The agency noted that police could deter criminal activity by increasing the perception that criminals will be caught and punished (NIJ, 2016). As law enforcement agencies, the target population for this research is uniquely positioned to influence the perception of the likelihood of a cyber actor being caught. As both the potential victim of a hacktivist perpetrated attack and a law enforcement agency who are empowered with a mission to pursue criminals, police agencies have a unique opportunity to influence defenses by leveraging technological mixed deterrence tactics (Bergal, 2017; Smith W, 2012).

A proactive approach to deterrence is what Freedman (2004) described as preemption. Following the Cold War and the collapse of the Soviet Union (U.S.S.R.), the strategic deterrence present through most of the Cold War era was based on equal strength on both sides. When erosion of one party occurred, it left one dominant superpower and several smaller pockets of anti-Western political groups leading to an era of *super-terrorism* (Freedman, 2004, p. 84). As the lone superpower, at the end of the Cold War, the U.S.became a prime target for terrorism, both physical and online. (Freedman, 2004). For example, the reaction to the first significant attack on the United States in this era by a foreign entity on September 11, 2001, caused the adoption of a new preemptive deterrence strategy focused on mitigating a threat before the threat can inflict substantial damage (Freedman, 2004).

In a February 2010 article in The Washington Post, retired Navy Vice Admiral and Director of National Intelligence, Mike McConnell, suggested that the only effective countermeasures against cyber-attacks include a mixture of deterrence and preemption (McConnell, 2010). McConnell (2010) suggested that preemptive action in cyberspace includes better sharing of actionable intelligence among both the public and private sector, taking defensive actions to respond to known threats, and implementing defensive tactics aimed at hardening infrastructure to make organizations a more difficult target for attack.

In a 2016 article in the International Journal of Computer Applications, Khadke and Madankar (2016) suggested a preemptive protection model aimed at defending against DDoS attacks through a combination of data flow inspection and data integrity checks. The remarks of Vice Admiral McConnell (2010) and the research conducted by Khadke and Madakar (2016) stress the relevance of preemption as a potential next-phase approach to deterrence in cybersecurity. Challenges increase when attempting to implement defensive tactics with rapid innovation in the commercial, criminal, and consumer technology spaces. The following section discusses the role of technology in a rapidly changing society and as a subset of society, police agencies, and officers. The following section explains how technology is changing society.

## Technology's Role in a Changing Society

Since 2000, the adoption of modern technologies by United States citizens has been exponential (Smith A., 2017). According to the Pew Research Center, adults' use of the internet in the United States has grown from 52% in the year 2000 to over 88% in 2016 (Smith A., 2017).

Smith (2017) found that access to broadband internet in homes over the same period rose from 1% to 73%. The use of social media has also risen among adults in the United States, from 5% in 2005 to 69% in 2016 (Smith A., 2017).

According to a report by the Pew Research Center (2018), the adoption of mobile technologies (smartphones, tablets, etc.) is equally as impressive as the increase in internet and social media. Between 2011 and 2018, the percentage of adults owning a smartphone has grown from 35% to 77% (Pew Research Center, 2018). Pew estimated that in 2018, 100% of 18 to 29year-olds in the United States own cell phones, with 94% owning a smartphone (Pew Research Center, 2018). According to Pew (2018), the only age demographic that does not breach the 50% mark of smartphone users is the population over the age of 65.

Chris Pemberton (2017), with global IT research firm Gartner, suggests that this phase of internet and smartphone adoption and increasing technical capability and dependency is only the beginning. Gartner estimated recently that by the year 2020, 100,000,000 consumers will have adopted augmented reality as a way to shop and that a majority of commercial interactions will use artificial intelligence, and have no human involvement on the part of the vendor. (Pemberton, 2017). The following section explains how the police force has evolved with technology to deter cyber-attacks.

### The Evolution of Police Force Technology Use

Although tradition and legacy models of policing may limit the overall potential impact of technology on law enforcement operations, the transformation and increasing dependency on technology by police are well supported in existing literature (Lum, Koper, & Willis, 2016). Unlike the days of traditional policing that consisted of patrolling neighborhoods, interacting with citizens, and physically looking for activities that may appear out of place or suspicious, the modern-day policing places increased technical demands and expectations on police. This a trend that has been growing for decades. Now policing includes departments finding and disrupting lone wolf or terrorist cells and searching for elusive online cybercriminals (Accenture, 2016).

Scholars studying the history of law enforcement in the United States typically divide law enforcement history into four eras: *political*, ranging from 1840-1930; *reform*, ranging from 1930-1970; *community*, from 1970-2001; and *the new era*, from 2001- present (Worrall & Schmalleger, 2013). Each era has provided new challenges as well as new technologies aimed at assisting police with these challenges (Worrall & Schmalleger, 2013). For example, Worrall and Schmalleger (2013) document that the first era (political) introduced notable communication advances, such as the telegraph and telephone.

Before the introduction of communication technologies, police, who found themselves in trouble or need of assistance, would attempt to draw attention to themselves by beating nightsticks against the ground or using loud rattles or whistles (Worrall & Schmalleger, 2013). The invention of the call box gave officers direct, immediate communication with the station at set intervals along the street. Communications technologies introduced both technological independence and dependence, through which officers became independent from the help of citizens but more dependent on the lifeline communication to the station personnel and fellow police officers (Worrall & Schmalleger, 2013).

Another technological innovation of the political era was the introduction of fingerprint identification. The FBI identification division began the collection of fingerprint records as early as 1924, with 800,000 submissions coming from the Leavenworth federal penitentiary (FBI, 2009). Before the advancement of fingerprint identification, criminal identification relied on eyewitness testimony or required an officer to witness the act (FBI, 2009). The introduction of fingerprint or biometric identification allowed the comparison of prints left at a crime scene against those of suspects for positive identification (FBI, 2009).

The reform era of policing witnessed further advancements in police technology, particularly in the area of communication. With the introduction of the one-way radio broadcast, the officer could be increasingly mobile in his newly issued automobiles and quickly receive calls for help from the station by tuning into the appropriate radio station on the in-car radio (Worrall & Schmalleger, 2013). The introduction of wireless one-way dispatch meant that although the call box was still used for communication from the officer to the station, frequent check-ins at the call boxes were less necessary because officers would receive updates and calls for help from the station before the next check-in (Worrall & Schmalleger, 2013).

After World War II, police adopted new technology in the form of two-way radio communication. Two-way communication allowed the officer to quickly communicate to the station, taking the first significant step in true mobility (Worrall & Schmalleger, 2013). Communication technology would continue to evolve through the rest of the reform era, with the form factor of radios shrinking dramatically into something that could be carried around by the officer when performing duties away from the car (Worrall & Schmalleger, 2013). The officer's ability to walk through the community while remaining connected has ushered in the community era of policing.

The adoption of commercial and technological innovations, such as personal computers and mainframes or servers, continued the theme of communication and identification advances (Chan, 2001). Through the adoption of technology over subsequent decades, officers could access vast amounts of information while communicating valuable information to counterparts across town or the country in a matter of minutes by using a mobile data terminal (MDT) (Chan, 2001). MDTs and laptop computers gave officers a distinct advantage when attempting to identify and apprehend criminals by detailing an offender's criminal past, frequented addresses, and known associates (Chan, 2001).

Identification was also significantly improved in the 1980s when the FBI's fingerprint repository was upgraded with the introduction of the Automated Fingerprint Identification System (AFIS) (FBI, 2009). AFIS enabled fingerprints lifted from a crime scene or from a perpetrator on the streets to be compared quickly to known prints using servers that could compare prints in a matter of minutes rather than the years it took for a trained fingerprint examiner to complete the same task (FBI, 2009). Modern technological advances have primarily been used by officers in the field when responding to a call and are becoming a defining element of an officer's everyday work leading to changes in the way officers approach duties and exercise discretion (Lum et al., 2016).

According to a 1998 report prepared for the National Institute of Justice, the workload that crime posed to the police in the late 1990s was five times higher than that in 1960, yet resource allocations failed to keep up with the increased work (NIJ, 1998). In an attempt to address the disparity between workload and assigned resources, law enforcement agencies began to drive technological changes and implementation on the basis of three imperatives (Chan, 2001). According to Chan (2001), the first imperative for the successful deployment of police technology is to improve efficiency and organizational legitimacy through the use of technology. The second imperative for the successful deployment of police technology is to ease both political and financial costs associated with providing police data to external entities (Chan, 2001). The third imperative to the successful deployment of police technology is to improve performance and efficiencies aimed at better service delivery to the general public (Chan, 2001).

In a 2003 essay, Steven Brandl described what research shows as an *information wave,* building up momentum, creating more demands on the police while also describing an increased likelihood of social disruptions (Brandl, 2003). The increase in social disruptions strains the police, who act as front-line representatives of the government and are often the first ones called when societal norms begin to deteriorate (Brandl, 2003). According to the 2015 report based on technology workshops conducted by the Police Executive Research Forum, police executives are significantly concerned that the inability of law enforcement agencies to adopt and protect their technology may result in an *undesirable future,* where criminals have a technological advantage over law enforcement agencies. Criminal having a technological advantage over law enforcement agencies can erode the public's trust in police effectiveness at enforcing the law (Silberglitt et al., 2015).

While the rate of adoption has been slower among some law enforcement agencies, law enforcement officers today rely on their devices including MDTs, handheld computing devices, and mobile AFIS devices to perform their daily tasks (Chan, 2001; Lum et al., 2016). The daily reliance on technologies, such as internet protocol-based communications to call for help, mobile identification to determine the legal status of an individual and mobile applications used to complete reports and obtain directions to mobile calls, has left some officers overly dependent on the technology (Chan, 2001; Lum et al., 2016).

**Police Reliance on Technology**

Lum, Koper, and Willis (2016) found that some officers were so reliant on technology that the police force lacked skills essential to policing, including navigation to calls for service without the use of GPS or other computer-aided navigation tools (Lum et al., 2016). A more recent report, released in 2015 by the President's Task Force on 21st Century Policing, described new and emerging technology as a shift in how police officers deliver their services to the community (Office of Community Oriented Policing Services, 2015). The report noted that while technology can play a crucial role in performing the work of policing with high efficiency, particular care should be taken to ensure that technology is not relied upon to the extent that it damages the relationship between the officer and the community served (Office of Community Oriented Policing Services, 2015). Simmons (2015) suggested that agencies must be cautious when adopting technologies to consider the concerns of the community over technology use in the police force (Simmons, 2015).

The problem of over-reliance on technology by police has been fueled primarily by nearly 25 years of issuing laptops and other electronic devices with the same critical importance as guns and badges (Lum, Koper, & Willis, 2016). This historical introduction of technology is evidenced by a 1998 quote from Dennis E. Nowicki, former Chief of Police for the Charlotte, North Carolina Police Department: “My vision is that when an officer comes through the academy, we give him his weapon, we give him his radio, and we give him his laptop computer” (NIJ, 1998, p. 13). The actual rate of adoption of technology by law enforcement agencies is missing from the literature, representing a significant gap in the current body of knowledge that is an intriguing area for future research.

The problem of reliance on technology is compounded by the recent adoption and movement toward Radio-Over-Internet-Protocol (ROIP) and Voice-Over-Internet Protocol (VOIP) in both critical communications and 911 emergency communications services. In the U.S., a multi-year, multi-million-dollar federal initiative created a nationwide wireless communication network dedicated to public safety users, known as FirstNet (First Responder Network Authority, 2016). In order for the general public to gain access to police, the national emergency number system known as 9-1-1 is undergoing a transformation to VOIP-based communications that offer greater interoperability and agility, known as Next Generation 911 (NG911) (Greenguard, Mullich, & Parch, 2016). Both FirstNet and NG911 communications are promising in scope and capabilities. However, both will be heavily relied upon by law enforcement and the public alike as a critical lifeline during emergency events and, even more critically, during significant incidents of civil unrest (Hawkins, 2013).

Many agencies will abandon legacy technologies that could act as a suitable backup and introduce resiliency because of cost concerns and regulatory requirements. Consequently, this compounds the problem of over-reliance on modern communication technologies (Hawkins, 2013). The Federal Communications Commission narrowband mandate in 2013 is an example of how regulatory requirements can impact police reliance on newer technologies (Federal Communications Commission, 2016). To meet new regulatory requirements, many law enforcement and public safety agencies are abandoning legacy radio systems for new, more advanced communications technologies (Hawkins, 2013). The migration to internet protocol-based communication systems introduces an attack surface to global cyber threat actors. Previously, law enforcement communications systems were off limits to hackers who would seek to disrupt public safety operations at a time of most critical need (Christensen, Caelli, Duncan, & Georgiades, 2010). The initial upgrade of legacy technologies is often viewed in a positive light until it is examined more critically. According to Hawkins (2013), agencies and officers become entirely dependent on new systems without the option to keep older systems to use as a backup. The next section will detail the background of existing cybersecurity frameworks.

## Background of Existing Cybersecurity Frameworks

Within the last ten years, progress has been made toward the development of cybersecurity frameworks and standards to guide organizations through implementing cybersecurity governance and controls to combat the negative impacts of a cyber-attack (Moraetes, 2018). Two of the frameworks, the ISO 27000 series of standards and the NIST Cybersecurity Framework, have emerged among the most widely known and accepted among the community of IT professionals (Moraetes, 2018). While the literature is limited related to the adoption of either of these frameworks in the law enforcement community, the literature does reveal the background of the frameworks along with some cited benefits and criticism related to their effectiveness and implementation limitations, as summarized below.

The ISO 27000 series, published by the International Organization of Standardization (ISO), was first published in the current format in 2005 (Palacios & Peterson, 2015). The series of standards provides guidance on assisting organizations with the management of all security assets (Bevan & Earthy, 2017). The series consists of over a dozen individual standards; the most relevant to this study are 27001 and 27002 (Bevan & Earthy, 2017).

ISO 27001 provides specifications for the establishment and management of an information management system within an organization (Bevan & Earthy, 2017). ISO 27002 relates directly to the selection and management of security controls within the context of the broader governance framework established in 27001 (Bevan & Earthy, 2017). At just over ten years old, the ISO 27000 series of standards are still in relative infancy with frequent updates, (most recently in 2018) but have already generated a fair amount of both praise and criticism from the IT community (Donaldson, Siegel, Williams, & Aslam, 2015).

Common praise for the ISO standards is based on the publishing organization's global reach, efforts to produce a common framework for organizations globally to strive toward, and the standard's flexibility, which are all critical factors given the global nature of the internet (Rukh & Malik, 2017). Common criticisms include that the ISO standards focus only on broad governance topics and not on specific technical controls that will translate into effective cybersecurity (Watson, Tellabi, Sassmannahausen, & Lou, 2017). An additional criticism is that the ISO standards are often viewed as a *pay to play* standard, requiring organizations to buy a copy of the standards themselves to view the changes, and pay third-party auditors to certify alignment with the standards (Cartwright, 2017).

Unlike the ISO 27000 series, the NIST Cybersecurity Framework is published by a U.S. government entity and is an open framework published online. While the framework is globally open, the focus of the framework is primarily to promote the protection of industries and interests in the U.S. national security and economy (NIST, 2018b). Initially published in response to U.S. Presidential Executive Order 13636 in 2013, the NIST Cybersecurity Framework version 1.1, was released in early 2018 (NIST, 2018b).

The NIST Cybersecurity Framework is divided into three components: the core, implementations tiers, and profiles (NIST, 2018a). The first component, the core, provides general activities and outcomes desired by an organization and primarily focuses on broader cybersecurity governance matters, such as ISO 27001 (NIST, 2018a). The second component, the implantation tiers, guide organizations by giving context to the organization's current cybersecurity maturity and offer a starting point for both governance and operational cybersecurity discussions (NIST, 2018a). The third component of the NIST Cybersecurity

Framework, the profiles, provide more specific guidance on identifying organizational priorities and improvement opportunities as they relate to cybersecurity (NIST, 2018a).

Similar to the ISO standards, the NIST Cybersecurity Framework is still new to the industry and has gained both support and criticism. Collective support for the NIST framework is that it fills a gap where previously there was little to no guidance specific to the organizational cybersecurity posture in the United States (Garlipp, 2015). A common criticism is that the NIST framework is optional, limiting adoption, and provides little opportunity for organizations to use the framework to manage their risk and determine how that risk relates to other organizations or industries (Copeland, 2017; Shackleford, Proia, Martell, & Craig, 2015).

Both the ISO 27000 series and the NIST Cybersecurity Framework are significant contributions to the broader cybersecurity community and are an excellent starting point in securing organizations against a cybersecurity attack. The praises and criticisms of both frameworks are fair, since they were introduced recently and are an initial attempt to address a very complex problem. Given additional time and refinement, there is reasonable support to suggest that the frameworks will achieve wider adoption and support (Donaldson, Siegel, Williams, & Aslam, 2015; Moraetes, 2018).

## Synthesis of the Literature

The literature reviewed as a part of this study included seminal works on topics such as civil disobedience (Thoreau, 1849) and deterrence (Hobbes & Gaskin, 1998), both of which contribute significantly to understanding the complex nature of hacktivism and the importance of the defense of law enforcement agencies in the United States. The literature documents the intimate relationship between America’s civil liberties and the exercise of the right to protest when citizens feel that an injustice has been done (Friedman, 2005). While law enforcement response to incidents of civil unrest is a necessary function of government as a means of restoring law and order, law enforcement actions taken to restore order may make police the target of retaliation by protesters.

The rapid adoption of technology among the U.S. general public, the evolution and rise of hackers coming to the aid of activists, and a growing dependency on technology by the police have created a potential for conflict and damage if appropriate mitigating steps are not taken. The ideas of adequately signaling the protesters and ensuring that the act hits the *sweet spot* of garnering attention are at the core of determining the success or failure of an act of civil disobedience. These ideas ensure that the act hits the *sweet spot* of garnering attention but not at the cost of garnering widespread rejection of the movement (Glaser & Sunstein, 2016). The two pillars of the theory on civil disobedience expose some potential opportunities for law enforcement to utilize deterrence or preemption in an attempt to disrupt the movement's likelihood of targeting police before any potential attack occurs (Coleman, 2014; Freedman, 2004; Glaser & Sunstein, 2016).

The idea that there is an intrinsic connection between the actions of the protesters and the police, as well as in the technology used on both sides of a protest, expose a few key points from the literature. First, theories surrounding civil disobedience and deterrence are equally valid and applicable when examining hacktivism and other forms of electronic civil disobedience. The literature demonstrates that the last 100 years have been filled with significant improvements in the way that law enforcement uses technology to accomplish their mission along with the rapid adoption of technology by the general public (Office of Community Oriented Policing Services, 2015). The advancement of technology, however, has come at a cost. For example, many officers and agencies have become dependent on technology to accomplish day-to-day functions (Lum, Koper, & Willis, 2016; Silberglitt et al., 2015; Simmons, 2015).

The failures noted in previous research methods include several significant gaps in the body of knowledge that exists regarding technology adoption rates by law enforcement agencies in the U.S., the capabilities of those organizations to protect against cyber-attacks, and the relationship between the police's dependency on technology compared to their civilian counterparts. The literature exposes that little formal or academic research has been performed regarding cybersecurity within the law enforcement industry as a whole. The gaps in the body of knowledge, if filled through proper research, could provide a clear and actionable model to state and local law enforcement agencies on how to protect their agency's technology proactively from the threat of a cyber-attack, particularly one perpetrated by hacktivists.

Current research only indicates the existence and motivation of hacktivism and that law enforcement will likely be a target of hacktivists, either directly or as collateral damage, but provides no solution for the problem (Amoroso, 2016; Bergal, 2017; FBI, 2015). While existing frameworks do exist to address cybersecurity governance and protections, most notably the NIST National Cybersecurity Framework and ISO 27000 series, there is little scholarly evidence or literature to suggest that either of these frameworks has made a direct impact on law enforcement agency cybersecurity. The threats faced by law enforcement agencies are similar to those faced by organizations in other industries. However, a lack of academic research specific to the law enforcement discipline and state and local government makes it difficult to assess the challenges an agency would face when attempting to apply an existing comprehensive framework to the unique challenges associated with defending a law enforcement agency against a hacktivist cyber-attack.

Additional research supports a growing dependency on the same law enforcement technology likely to be in the crosshairs of a hacktivist during a period of civil unrest. However, the existing literature lacks the level of specificity necessary to identify specific systems and defensive techniques that may be employed to mitigate such a risk (Byrne & Marx, 2011; Chan, 2001; Lum, Koper, & Willis, 2016). The previous research methods and existing cybersecurity frameworks do not account for the consensus of experts who have faced problems associated with the protection of law enforcement technology, worked to overcome challenges, and can contribute to a model aimed at solving the specific problem, which is the focus of this research. This research is focused on the development of a model that may be employed by the U.S., state, and local law enforcement agencies to protect their agency's critical IT infrastructure through the use of techniques aimed at disruption of the tactics typically employed by hacktivists and actions with the intent of deterring attacks in the first place. There is no literature to support the application of existing cybersecurity frameworks, namely, the NIST National Cybersecurity Framework or ISO 27000 series, as a method of deterrence to protect specifically against the holistic agency impacts of hacktivist attacks on agency public opinion, department operations, and system availability. This study will not only advance the research in U.S. critical infrastructure protection but also provide a comprehensive model for implementation by law enforcement agencies to protect from the adverse effects of a hacktivist cyber-attack.

## Summary

The literature review presented in the first two chapters of this dissertation is the result of an exhaustive review of the literature regarding a variety of topics related to the history, theories, and police response to technology-based civil disobedience in the U.S. Included is an examination of literature related to the role of technology on societal change and law enforcement’s adoption and growing reliance on technology. Each of the topics included in this literature review contributes substantially to understanding the impact of hacktivist attacks on law enforcement agencies and the potential detrimental effects caused by a failure to defend against cyber-attacks appropriately.  Chapter Three explains in detail the method used to conduct the research study.

# CHAPTER 3. METHODOLOGY

## Introduction

The general problem addressed by this study is that the combination of law enforcement's growing dependency on technology and the increasing threat posed by hacktivism has created a potential crisis leaving state and local law enforcement's response capabilities in a vulnerable state (Bergal, 2017; Amoroso, 2016; Lum, Koper, & Willis, 2016). Events of civil disobedience, witnessed since 2010, are changing the nature, identity, and effectiveness of hacktivism in disrupting technologies critical to state and local law enforcement operations (Coleman, 2014). The specific problem is that the effectiveness of hacktivists and state and local law enforcement's growing dependency on technology has created a more significant attack surface that police agencies are increasingly unprepared to protect (Newcome, 2015).

The purpose of this qualitative Delphi study was to develop a proactive, defensive model by examining the perceptions and experiences of law enforcement technology experts in the U.S. to identify consensus around the primary influencing factors in the hacktivist targeting of law enforcement agencies and the effectiveness of defensive tactics used by law enforcement agencies in mitigating the impact of hacktivist cyber-attacks.

This study employed a mixture of online and phone interviews of an expert panel comprised of five state and five local U.S. law enforcement technology experts currently holding a leadership position with influence over technology application and strategy. Chapter Three explains in detail the method used in the research study. In the following sections, the target population, sampling, and procedures are detailed, data collection methods are explained, and ethical considerations are considered.

## Design and Methodology

This study employed a qualitative Delphi method to examine the perceptions and experiences of law enforcement technology experts in the U.S., to identify areas of consensus around the primary influencing factors on the hacktivists' targeting of law enforcement agencies, to determine the effectiveness of defensive tactics in mitigating the impact of hacktivist cyber-attacks on department operations, and to create a law-enforcement-focused proactive defensive model.

The Delphi technique was developed in the 1950s by the RAND Corporation in response to an identified need for the U.S. military to develop consensus quickly among experts to forecast the future impact of technology on warfare during the challenging Cold War era (RAND Corporation, 2016). The Delphi method is well suited to build consensus among industry experts through the employment of interviews delivered in multiple iterations, which allows the experts to review the responses of their peers and refine judgments throughout the process (Chia-Chien & Sandford, 2007).

Because of the nature of hacktivism, as a relatively new and emerging threat, the expertise surrounding practical and effective defensive measures to protect agencies against potential adverse outcomes is held almost exclusively by subject matter experts within the law enforcement technology community. The Delphi method is particularly well suited for this study because of the lack of a defined, actionable model to deter cyber-attacks against the police and the lack of ability to gauge consensus and forecast potential future impacts (Chia-Chien & Sandford, 2007). The following section explains the population of experts in the study.

## Participants

In 2008, state and local law enforcement agencies numbered nearly 18,000, representing over 1.1 million sworn police personnel according to the last published census conducted by the U.S. BJS (United States Bureau of Justice Statistics, 2011). The police force charged with enforcing law, includes local police departments, constables, and county or parish sheriff's offices as well as state police and highway patrol agencies (U.S. DOJ, 2016). In many small and large communities alike, the police are the most visible part of the government and may be the first to be impacted by actions taken against the government, including forms of electronic civil disobedience.

For this study, the population consisted of technology experts who hold a leadership position in the application and strategy of technology within state and local law enforcement agencies. The law enforcement technology leaders in the U.S. are presented with the same challenges faced by other IT leaders on a daily basis, including a technological failure that may potentially cause the loss of life for a citizen in need or, even, a co-worker in the line of duty. Because of their experience in maintaining critical systems and their close connection to department operations, the identified technology leaders represent the industry experts who best understand and can best respond to the business problem as presented.

The sample for this study was comprised of ten experts, including five state and five local law enforcement officials in a leadership position holding influence over technology strategy within a state or local law enforcement agency in the United States. Experts were solicited by invitation to participate in the study based on their role in the organization related to technology strategy, job description, and familiarity with law enforcement industry cybersecurity regulations and standards.

While there is little consensus on the number of experts needed to conduct a Delphi study, research suggested that the optimum number of panel participants is in the range of seven to twelve (Phillips, 2000). Five experts from each jurisdictional category were selected to gauge consensus equally among local and state jurisdictions based on a 10% representation of U.S. states.

The ten experts were selected based on specific criteria. Each expert currently holds a decision-making position regarding the application and strategy of technology within a law enforcement agency, has a minimum of five years of experience in a decision-making capacity, and demonstrates an advanced level of understanding and experience in enforcement or influence of the FBI Criminal Justice Information Services Security (CJIS) policy, which represents the law enforcement industry's cybersecurity regulatory requirements. The group of experts comprised five state and five local law enforcement officials with the qualifications noted above. The experts were each in a leadership position asserted some authority over the technological strategy within a state or local law enforcement agency in the United States.

Participants with expertise in guiding IT and information security strategy within the U.S. law enforcement agencies have diverse backgrounds. Education level, years of service, and specific training vary significantly among law enforcement technology leaders. For instance, even among larger jurisdictions, technology leaders may be sworn law enforcement officers with the vast majority of their experience being on the street and dealing with the physical elements of unrest making the expert no less qualified to provide input on hacktivism effects and possible mitigations than civilian counterparts in other agencies. Conversely, while civilian law enforcement leaders may have IT degrees and experience, most civilian law enforcement technology leaders lack any significant experience in dealing with crime and unrest in the streets.

In smaller jurisdictions, the technology expert holding a leadership role may be an officer with two concurrent roles, namely, managing technology while also providing regular police services. An officer, who is active in policing and as a technology leader, brings the unique perspective of performing both roles in an instance of hacktivism and can address the physical and cyber threats simultaneously.

A significant benefit of the Delphi method is a technique to gauge the consensus of a group with diverse backgrounds to find common perspectives and approaches to a problem. The researcher determined that creating a stringent, static test of qualifications would potentially eliminate critical input from agencies not fortunate enough to have technology leaders with the selected qualifications. Law enforcement is often plagued by anti-intellectualism, which extends to management of IT through the organizational view of IT as a support function instead of a core component of service delivery (Foley, 2010). Approaching technology as a support function creates a problem when identifying duly qualified technology experts in comparison to other industries in regard to the heterogeneous makeup of technology leaders within the discipline. The identification of experts with the appropriate understanding of law enforcement operations, unique technological challenges, broader IT trends, and potential policy implications require more thorough analysis than the conventional measures of IT qualification. For this study, an analysis was conducted of the duties performed delineated by job descriptions and title, educational background, and involvement in the creation, influence, or implementation of national cybersecurity policy by each expert. The experts selected for this study have a combined 42 years of higher education, 171 years of experience in the law enforcement field, and143 years were explicitly dedicated to law enforcement technology management. The analysis completed by the researcher exposed enough detail to determine qualifications, leading to the selection of the correct experts for this particular study.

## Setting

The researcher assembled the setting for the panel of experts using a LinkedIn group, which the researcher administers. Members were invited to participate in the study based on their role in the organization as it relates to technological strategy, job description, and familiarity with law enforcement industry cybersecurity regulations and standards.

According to the Microsoft 2017 annual report, LinkedIn is a professional network representing over 500 million users (Nadella, 2017). The network contains names, contact information, and basic curriculum vitae information, which can validate the expert's background and experience. This information is important in conducting a Delphi study. The selection of LinkedIn as the setting for this research was validated, at least in part, by the research conducted by Lops, De Gemmis, Semeraro, Narducci, and Musto (2011), which analyzed LinkedIn user profiles and determined that the network is a very useful professional networking tool and that users regularly update their profiles. The access to timely, accurate biographical data as well as contact information on potential experts made the selection of LinkedIn as the setting for this study is most appropriate.

## Analysis of Research Questions

The following research question directed and narrowed the literature review, research methodology, and the analysis of data:

> RQ: What better model of cyber security defensive tactics could be developed to prepare U.S. state and local law enforcement agencies to defend against hacktivist cyber-attacks

in the future, as perceived by United States state and local law enforcement technology experts?

With the focus of identifying a model based on the perception and experiences of an expert panel, the research question in this study is well suited for a qualitative Delphi research method, which focuses on measuring consensus among industry experts through the employment of interviews delivered in multiple iterations (Chia-Chien & Sandford, 2007).

The researcher collected data for this study from law enforcement technology experts using a multi-round, iterative series of questionnaires delivered by a combination of phone and email interviews. Round 1 consisted of an open-ended questionnaire (see Appendix A), which was formulated by the observations of the researcher, the theoretical orientation of the study, and scholarly support obtained through the literature review as shown in chapter two. The topics in the Round 1 questionnaire examined the experts' perspectives on the likelihood that cyber-attacks on law enforcement were increasing or are likely to increase in the future, what factors contribute to the targeting of law enforcement, and what types of systems or department systems most likely impacted by a cyber-attack. Experts were also asked for their perspective on the role deterrence plays in curbing attacks and what challenges law enforcement agencies face when protecting IT systems. The questions in Round 1 were responsive to the research question, establishing a baseline determinant of the experts' experiences and observations on hacktivist attacks on law enforcement. The theoretical orientation of the study guided the creation of the questions in Round 1. The theoretical orientation is comprised of the theories of civil disobedience, social movement theory, and measurement of deterrence theory and how their applications are effective in preventing future hacktivist cyber-attacks. The Round 1 questionnaire served as the basis for identifying patterns and themes in the study as well as the development of questions included in the Round 2 questionnaire.

Along with the Round 2 questionnaire, each expert also received the Round 1 responses, as summarized by the researcher, to begin the consensus-building process. The Round 2 questions required additional information on areas of consensus measured in Round 1. In some cases, the experts were required to explain the rationales for the rating given. After completion of Round 2, the researcher analyzed the results of the structured questionnaire with the same method as the Round 1 results with areas of consensus provided to the panel for review and consideration in Round 3. More themes were developed from a combination of the results of Rounds 1 and 2. These themes were presented to the panel in the Round 3 questionnaire.

Round 3 used the list of items for which consensus was achieved to give the experts a final opportunity to revise their opinions, introduce new information, and indicate the level of agreement with the identified themes developed in Rounds 1 and 2. Using measures of central tendency, the researcher determined that no additional rounds were required due to complete consensus and data saturation. The researcher coded and analyzed the results from each round, as described above, using Microsoft Excel and Nvivo 11. The coding process focused on the development of themes based on expert consensus. The researcher used measurements of central tendency in the analysis of Round 3 results and determined that both complete consensus and data saturation had been achieved, and no additional rounds were required (see Appendix B for guiding interview questions). The same questions, approved by the Capella University institutional review board (IRB), were asked in each round, which had been approved by the IRB.

In this study, the researcher's role was as an instrument to facilitate the iterative interviews, analyze responses for trends and patterns until data saturation, protect the confidentiality of participants, and propose a model that does not currently exist, based on the consensus identified in the research. The researcher has twenty years of experience in public safety, dating back to the mid-1990s, including over ten years of direct experience in secure public safety technology solutions. The last five years of experience have been as a Chief Information Security Officer for state law enforcement, which has included a significant response to hacktivist attacks on law enforcement. This direct experience has provided the researcher with a unique perspective on the challenges that public safety agencies face on a daily basis when managing cybersecurity, technology, and the skills necessary to carry out the role required by this study.

## Credibility and Dependability

The credibility of any academic research is determined by the overall contribution to the body of knowledge and the value of the research design, implementation, and analysis of the research (Cope, 2014). Solving the problem of hacktivists' effectiveness and the growing dependency on technology by state and local law enforcement creates a more significant attack surface, which police agencies are increasingly unprepared to protect (Newcome, 2015). This research has the potential to make significant contributions to the body of knowledge and to have a significant impact on the adoption and protection of law enforcement technology in the U.S.

A qualitative Delphi method is particularly well suited to result in a credible and dependable outcome since the intent of the research is to develop a defensive model based on the perceptions of law enforcement technology experts (Cole, Donohoe, & Stellefson, 2013). The anonymity of expert panelists not only protects the identities of participants but also allows unbiased answers to questions without fear of influence or *groupthink*, all of which contributes to the dependability of the study (Dabbagh & Lee, 2014). The fact that the Delphi method's dependability relies on the quality of opinions provided by the experts is noteworthy. For this study, the researcher conducted a thorough analysis of the duties performed, typically indicated by job descriptions and title, educational background, and involvement in the creation, influence, or implementation of national cybersecurity policy by each expert to ensure a dependable and reliable outcome. The experts selected for this study have a combined 42 years of higher education, 171 years of experience in the law enforcement field, and 143 years explicitly dedicated to law enforcement technology management. The analysis completed by the researcher exposed enough detail to determine qualifications leading to the selection of the right experts for this particular study.

While the dependability of this research as designed can only extend to law enforcement agencies within the United States, it is not unreasonable to conclude that the global nature of the internet and technology might make the resulting model applicable in international agencies. With the appropriate modifications, this research could be conducted with agencies in a particular jurisdiction with very dependable results based on the completeness of the research design and careful application (Cope, 2014).

## Data Collection

The researcher collected data from ten law enforcement technology experts using a multi-round, iterative series of questionnaires delivered by a combination of phone and email interviews. Round 1 consisted of an open-ended questionnaire that formed the basis for identifying patterns and themes. After Round 1, the researcher analyzed the results to identify themes emerging from the responses. The researcher used the results and themes to formulate a structured questionnaire for the experts to answer in Round 2. When presented with the Round 2 questionnaire, each expert also received the Round 1 responses, as summarized by the researcher, to begin the consensus-building process.

Round 2 questions required expansion on areas of consensus measured from Round 1. In some cases, the experts were required to express the rationale for their ratings. Upon completion of Round 2, the results of the structured questionnaire were analyzed with the same method as in Round 1, with areas of consensus provided to the panel for review and consideration in Round 3. More themes were developed from a combination of Rounds 1 and 2.

In Round 2, the list of items for which consensus was achieved was provided to the panel to give the experts a final opportunity to revise their opinions, introduce new information, and indicate the level of agreement with the identified themes developed in Rounds 1 and 2. The researcher used measurements of central tendency to determine that complete consensus and data saturation had been achieved, and no additional rounds were required. No new information was discovered. The researcher analyzed and developed the themes into a model in the following section.

## Data Analysis

For this study, the measurement of consensus was based on a combination of counts of common responses and measurement of central tendency. The researcher used the methods identified as a determinant of consensus; the collected data is presented in Chapter 4 as important themes determined primarily by the measures of central tendency, common to the Delphi technique (Chia-Chien & Sandford, 2007). Through the examination of the collected data and the areas of consensus reached by the expert panel, the research resulted in a more explicit model of future cybersecurity defensive tactics that law enforcement agencies can employ when preparing an agency for incidents involving hacktivist cyber-attacks.

In this study, the researcher's role was to facilitate the iterative interviews, analyze responses for trends and patterns until data saturation, protect the confidentiality of participants, and propose a new model based on the consensus identified in the research (see Appendix B for guiding interview questions). The same questions were asked in each round, an approach that was approved by the Capella University IRB.

## Ethical Considerations

The first ethical consideration is that data collection for this study began with approval from the Capella University Institutional Review Board. The second ethical consideration is that this study was limited to determining the consensus of state and local law enforcement experts in the U.S. and will not include the perspective of international, federal, or tribal police agencies. Because of the significant differences in politics and applicable laws between criminal justice entities and jurisdictions, applying the results of this study outside of its intended scope is not appropriate.

The third ethical consideration is that the underlying events in the vast majority of law enforcement-involved hacktivist actions are often high profile and politically charged, which may limit some participation by otherwise knowledgeable experts. Local policies may restrict specific information regarding defensive measures and tactics that may reveal key system vulnerabilities. The fourth ethical consideration is that this researcher has extensive experience in the field of law enforcement technology and cybersecurity, which has the potential to introduce bias into the study. The researcher controlled bias by avoiding experts from the same geographical area (state) as the researcher to avoid researcher and participant sharing common experiences tied to a particular event. The fifth ethical consideration is that, due to the concerns associated with the third ethical consideration, protection of the study participants identities and responses is crucial. The details associated with the protection of this information are detailed below.

### Protection of Participants

Maintaining confidentiality in this research study was critical because of the revealing nature of questions posed regarding past attacks and possible vulnerabilities in current law enforcement systems. The researcher used multiple methods to maintain participant confidentiality. Each participant method is explained below.

The first method used study codes on completed questionnaires. The researcher maintained a separate encrypted document that listed the study codes and how they represented participants' identifying information. The researcher will preserve they key to this encrypted document and will access the document as necessary. The completed questionnaires were stored in a separate, secured encrypted drive. At the completion and final publishing of the research, these encrypted drives will be locked for seven years, as required by the IRB, and then destroyed.

## Conclusion

Chapter Three presented a detailed outline of the methodology of this research study. Chapter Four presents the findings of this study, including a detailed analysis of each theme identified through the course of the study. From the detailed analysis of the identified themes gaining consensus among the experts, a defensive model responsive to the research question was developed and is presented in Chapter Five.

# CHAPTER 4. RESULTS

## Introduction

The general problem addressed by this study is that the combination of law enforcement's growing dependency on technology and the increasing threat posed by hacktivism has created a potential crisis, leaving state and local law enforcement response capabilities in a vulnerable state (Amoroso, 2016; Bergal, 2017; Lum, Koper, & Willis, 2016). Events of civil disobedience, witnessed as early as 2010 through the present day, are changing the nature, identity, and effectiveness of hacktivism to disrupt technologies critical to state and local law enforcement operations (Coleman, 2014). The specific problem is that the effectiveness of hacktivists and the growing dependency on technology by state and local law enforcement has created a more significant attack surface that police agencies are increasingly unprepared to protect (Newcome, 2015).

The purpose of this qualitative Delphi study was to develop a proactive defensive model by examining the perceptions and experiences of law enforcement technology experts in the U.S., to identify consensus around the primary influencing factors on hacktivist targeting of law enforcement agencies, and to determine the effectiveness of defensive tactics used by law enforcement agencies in mitigating the impact of hacktivist cyber-attacks.

The research question for this study is presented below:

RQ. What better model of cyber security defensive tactics could be developed to prepare U.S., state, and local law enforcement agencies to defend against hacktivist cyber-attacks in the future, as perceived by United States, state, and local law enforcement technology experts?

While developing a model of cybersecurity defensive tactics responsive to the research question, the researcher employed a mixture of online and phone interviews of an expert panel comprised of five state and five local law enforcement technology experts currently holding a leadership position with influence over technology application and strategy. Data was collected from experts over three iterative rounds of questionnaires that identified themes gaining consensus among the experts. The themes gaining expert consensus were compared against the literature to identify the themes as either new or supported by existing research. The outcome of this study is a model that has been developed based on the consensus of law enforcement technology experts that may be employed by U.S. police agencies to improve the overall law enforcement defensive cybersecurity posture in the United States. The remainder of Chapter Four is organized to present the data collection results, data analysis and results, and a summary of the findings.

## Data Collection Results

Data were collected from ten law enforcement experts, using a multi-round iterative series of questionnaires delivered by a combination of phone and email interviews. An examination of the demographics of the technology experts selected for this study revealed the following details: six of the ten participants work in U.S. jurisdictions in large states, defined as having a population in the top 1/3rd of all states; three participants worked for jurisdictions in medium population states (within the top 2/3rd of all states but outside the top 1/3rd); and one participant works for a jurisdiction in a small population state (in the bottom 1/3rd of all states). The average number of years of law enforcement experience among the experts was 16.5; the lowest number of years was seven. When the total years of experience supporting law enforcement technology were calculated, the average dipped slightly to 13.9 and the lowest number of years was six. Each expert currently holds a position with leadership or decision-making capacity regarding technology in a state or local jurisdiction.

Each technology expert had experience as an influencer, enforcer, implementer, or combination thereof with the national CJIS Security Policy. Each technology expert had some level of higher education, with all but three possessing a four-year undergraduate degree, one of whom completed two years of college while two held a Master of Science degree. Half of the participants (50%) had dealt with an incident of hacktivism targeting or attacking a law enforcement agency. The characteristics of each participant are shown below, using a participant code:

S1 is a 20-year veteran of law enforcement in a medium population state. Fourteen years of this 20-year career has been dedicated to supporting law enforcement technology. S1 holds a B.S. in Criminal Justice, and Accounting, and had no experience handling an incident of hacktivism against a law enforcement agency. S1 had experience as an influencer, enforcer, and implementer of CJIS Security Policy.

S2 is a 20-year veteran of law enforcement in a large population state, all of which has been dedicated to supporting law enforcement technology. S2 holds a B.S. in Criminal Justice and Information Technology, has experience handling an incident of hacktivism against a law enforcement agency, and has experience as an enforcer and implementer of CJIS Security Policy.

S3 is a seven-year veteran of law enforcement in a medium population state. Six years of this career have been dedicated to supporting law enforcement technology. S3 holds an M.S. in Business and Information Technology but had no experience handling an incident of hacktivism against a law enforcement agency. S3 is experienced as an influencer, enforcer, and implementer of CJIS Security Policy.

S4 is a 22-year veteran of law enforcement in a large population state all of which has been dedicated to supporting law enforcement technology. S4 holds a Bachelor of Science, has handled an incident of hacktivism against a law enforcement agency, and has experience implementing CJIS Security Policy.

S5 is a ten-year veteran of law enforcement in a small population state, six years of service dedicated to supporting law enforcement technology. S5 holds a Bachelor of Science in mechanical engineering, had experience handling an incident of hacktivism against a law enforcement agency, and is experienced as an enforcer and implementer of CJIS Security Policy.

L1 is a ten-year veteran of law enforcement in a large population state, all of which has been dedicated to supporting law enforcement technology. L1 holds a Bachelor of Science in electrical engineering, had experience handling an incident of hacktivism against a law enforcement agency and is experienced as an implementer of CJIS Security Policy.

L2 is a 20-year veteran of law enforcement in a large population state, dedicated to supporting law enforcement technology. L2 holds a Bachelor of Science in Organizational Communication and had no experience handling an incident of hacktivism against a law enforcement agency, but has experience as an influencer and implementer of CJIS Security Policy.

L3 is a 20-year veteran of law enforcement in a medium population state. Twelve years of this career has been dedicated to supporting law enforcement technology. L3 holds a Bachelor of Science in Administration of Criminal Justice and has no experience handling an incident of hacktivism against a law enforcement agency but has field experience as a law enforcement officer and as an implementer of CJIS Security Policy.

L4 is a 31-year veteran of law enforcement in a large population state. Twenty-two years of this career has been dedicated to supporting law enforcement technology. L4 completed two years of collegiate coursework and had no experience handling an incident of hacktivism against a law enforcement agency, but had field experience as a law enforcement officer and as an influencer and implementer of CJIS Security Policy.

L5 is an 11-year veteran of law enforcement in a large population state, dedicated to supporting law enforcement technology. L5 holds a Master of Science in Information Technology and Information Security, has experience handling an incident of hacktivism against a law enforcement agency, and has experience influencing and implementing CJIS Security Policy.

Round 1 consisted of an open-ended questionnaire used as a basis for identifying patterns and themes. After Round 1, results were analyzed to identify emerging themes from the responses and were used to formulate a structured questionnaire for Round 2. When given the Round 2 questionnaire, each expert also received the Round 1 responses, summarized by the researcher, to begin the consensus-building process.

Round Two's questions required expansion on areas of consensus measured from Round 1. In some cases, the experts were required to express the rationale for their ratings. Upon completion of Round 3, the results of the structured questionnaire were analyzed. When presented with the Round 3 questionnaire, each expert also received the Round 2 responses, as summarized by the researcher, to continue the consensus-building process. More themes were developed from a combination of Rounds 1 and 2.

Round 3 presented the list of items on which consensus was achieved to the panel to afford the experts a final opportunity to revise their opinions and indicate the level of agreement with the identified themes developed in Rounds 1 and 2. The researcher used measurements of central tendency to complete consensus, and data saturation was achieved. No additional rounds were required, and no new information was discovered. The themes were analyzed and developed as presented in the following section.

## Data Analysis and Results

For this study, the measurement of consensus was based on a combination of counts of common responses and measurements of central tendency. The researcher used the methods identified as a determinant of consensus. The collected data is presented in the findings section of this chapter as important themes that focus primarily on the measures of central tendency, common to the Delphi technique (Chia-Chien & Sandford, 2007). Through the examination of the data collected and areas of consensus reached by the expert panel, the research resulted in a more explicit model of future cybersecurity defensive tactics that could be employed by law enforcement agencies when preparing an agency for incidents that involve hacktivist cyber-attacks.

The research data obtained from the expert panel responses to the interview questions were initially analyzed for trends and patterns, which were later organized into themes that were presented to the experts to gauge consensus and elicit additional details that could contribute to the identified themes. The analysis was completed by evaluating text responses for themes, based mainly on word counts performed with the assistance of the NVivo 11 software, written and supported by QSR International. Responses in Rounds 2 and 3 were evaluated for measures of central tendency on agreement among experts to determine consensus using Microsoft Excel (see Appendix B for guiding interview questions).

### Results

Consistent with the Delphi method, the research in this study elicited responses to the questions presented to the experts in the iterative multi-round process. This section presents the expert panel's responses and themes derived from the data collected through a combination of tables, figures, and narratives.

Table 1

*Contributing Factors to Hacktivists targeting Law Enforcement Agencies by number of experts*

| **Contributing Factor** | **Number of Experts Identifying** |
|---|---|
| Controversial Incidents | 6 |
| Media/Public Sentiment | 5 |
| Political/Social Issues | 4 |

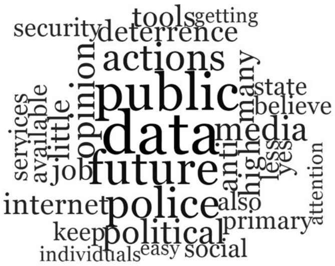

*Figure 1.* Word cloud analysis of Round 1 Q1 responses

The analysis of the expert responses to the question regarding the primary factors that contribute to hacktivist targeting of law enforcement revealed a clear theme: the role of media coverage, public sentiment, and broader political and social issues in determining whether an agency is likely to be targeted by a hacktivist attack. An additional theme was also identified, indicating that law enforcement agencies (LEAs) are mostly unprepared to defend against an attack, making them easy targets for hackers.

**Theme One: United States law enforcement agencies should actively manage the message and public perception surrounding controversial law enforcement incidents**

Nine of ten experts identified media coverage, public sentiment, and significant sociopolitical issues as significant contributors to an law enforcement agency being targeted by hacktivists and significant factors in the overall rise in hacktivist activities across the U.S. The expert L1 shared experience that suggested high-profile police-related incidents increase the likelihood of law enforcement being targeted by cyber actors in the future, in a sort of digital retribution for perceived injustices.

Expert S2 highlighted the role of digital media platforms in making potentially controversial incidents that would otherwise be restricted to local audiences draw global attention. The experts were asked to provide potential defensive tactics in response to the suggestion that agencies should work to manage the message and public perception of the law enforcement response to an incident. Seven of ten experts suggested that proper planning, establishing relationships, and active engagement play an important role in preventing or mitigating a hacktivist attack. Experts felt the need to control the message was even more critical following a high profile, controversial incident. According to the panel, because of the unpredictable nature of law enforcement incidents, a controversial event could occur at any time, so proper planning and engagement are vital.

From the next question, seeking the experts' perceptions of what types of systems were most likely to be impacted in the event of a hacktivist attack on a U.S. state or local law enforcement agency, another clear theme emerged, focused on public-facing (internet-accessible systems) communication systems because of their critical role in department operations and records management systems because of the sensitivity of the data they contain.

### Theme Two: United States law enforcement agencies should focus security efforts on critical or sensitive public-facing systems first

Eight of ten experts suggested systems that are internet-accessible or *public facing* posed the most significant risk of being targeted in the event of a hacktivist attack. Of particular concern were systems either critical to department operations, such as communications, or systems containing sensitive data, such as records management systems. Expert L5 said, “I think that public-facing websites are most likely to be impacted, followed by attempts to reveal personal information.”

Expert L2 offered a similar response to the response offered by L5, suggesting that websites were not the only systems likely to be impacted, but also any system that is public facing. Internet-accessible systems are typically configured in a demilitarized zone of the agency network for ease of use and access by legitimate customers. While convenient, an internet-facing configuration allows for a much more simplistic approach to exploiting vulnerabilities and gaining access and utilizing compromised credentials.

When asked about defensive tactics to protect public-facing systems, the experts suggested a variety of technical solutions, including firewalls, vulnerability scanning, advanced authentication, intrusion prevention, and encryption. The majority of experts suggested limiting public access to sensitive systems entirely through the use of dedicated or virtual private networks or IP address filtering.

The expert panel was asked to share perceptions regarding the role that deterrence plays in curbing attacks by hacktivist actors. Over half of the experts agreed that the successful arrest or prosecution of hacktivists targeting LEAs would likely play a role in curbing future attacks, exposing another theme: that an increase in the successful prosecution of cyber threat actors could play a role in the deterrence of future potential actors.

### Theme Three: United States law enforcement agencies should advocate for an increase in the investigation, pursuit, arrest, and prosecution of cyber threat actors as a method of deterrence

Six of ten experts believed that an increase in the arrest and prosecution of hackers would act as a deterrent to future potential hacktivists. None of the remaining experts suggested that an increase in prosecution would be useful. Two of the experts felt that successful pursuit and prosecution of such actors would be challenging without significant changes, while two others focused on technical deterrents that could play a role in preventing future attacks.

Expert S2 stated that "successful prosecution is key to any deterrence." Expert L3 suggested that deterrence was likely "only when major arrests take place or special focus is taken on the perpetrators". Law enforcement agencies play a role unique to most organizations regarding the use of prosecution as a type of deterrent. Not only are police agencies likely to become victimized, just like any organization, but what makes law enforcement agencies unique is the role of pursuing cybercriminals and increasing the likelihood the hacker will be caught and brought to justice for their actions.

When asked to propose actions agencies could take to increase the likelihood of successful arrest and prosecution, the experts suggested that agencies advocate for legislative changes to existing laws, strengthen penalties for cybercrimes, invest in investigative resources and staffing as well as restricting traffic to agency technology assets using U.S.-based IP addresses to increase the likelihood of successful prosecution in the event of an attack.

Finally, the panel was asked to identify the most significant barriers in protecting IT systems within U.S., state, and local law enforcement agencies. A word cloud analysis of responses to this question is presented in Figure 2.

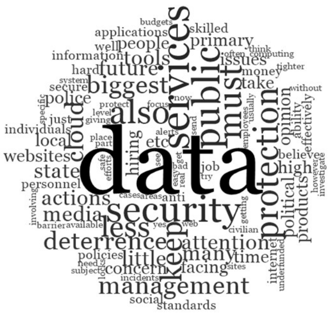

*Figure 2.* Word cloud analysis of Round 1 Q5 responses

From the analysis of the question regarding the most significant barriers in protecting IT systems, a few clear suggestions emerged with majority consensus: administrative and management limitations, such as budget, staffing, and training, all present significant challenges to agencies when defending against cyber-attacks. The concepts obtained from the data analysis were consolidated and are presented as Theme Four below.

**Theme Four: United States law enforcement agencies should focus on optimization of time, money, skills, people, and processes to overcome the most significant defensive challenges**

Eight of ten experts agreed that less than appropriate budget allocations, staffing issues, and lack of skilled personnel presented the most significant barriers when attempting to protect law enforcement agencies from the effects of cyber-attacks. While most cybersecurity efforts focus on the technology, many of the most significant progress in the cybersecurity field may be addressed through proper training, responsibility assignments, and other administrative controls. When asked to present the most significant barriers faced by law enforcement in agency defense expert L2 stated simply: “Time, money, and expertise”.

Expert L5 exposed an administrative challenge in recruitment and retention of skilled workers unique to law enforcement agencies by stating that, “Too often, law enforcement is reluctant to rely on civilian employees, however often the individuals who are best suited for IT tasks are not ideal law enforcement candidates.”

When requested to provide mitigating tactics in Round 2, the expert panel suggested the development of formal training programs and partnerships with local schools and colleges as methods to increase the cybersecurity workforce within law enforcement. The experts suggested an emphasis on cybersecurity as a core component of the organization and increased education of all stakeholders, to include executives and human resources, as ways to increase the priority placed on cybersecurity within the broader agency mission.

Each of the themes identified above was tested for consensus and experts were asked to provide additional specific defensive tactics that may contribute to a defensive model and refine the identified themes. The test used to determine consensus required each expert to rate their level of agreement with each theme on a scale of 1-5 (1 indicating strong disagreement and 5 indicating strong agreement). A summary of the measurements of consensus for each theme are detailed in Tables 2-4 below:

Table 2
*Average expert score indicating consensus – Theme 1*

| **Contributing Factor** | **Average Expert Score (Scale of 1-5)** |
|---|---|
| Media/Public Sentiment | 4.1 |
| Reaction to controversial incidents | 4.3 |

Table 3
*Average expert score indicating consensus – Theme 2*

| **Department System/Process** | **Average Expert Score (Scale of 1-5)** |
|---|---|
| Public-Facing Systems | 4.7 |
| Communications systems | 4.0 |

Table 4
*Average expert score indicating consensus – Theme 3*

| **Department System/Process** | **Average Expert Score (Scale of 1-5)** |
|---|---|
| Role of Arrest/Prosecution as a deterrent | 4.0 |

Table 5
*Average expert score indicating consensus- Theme 4*

| **Identified Barriers** | **Average Expert Score (Scale of 1-5)** |
|---|---|
| Budgetary Restraints | 4.0 |
| Staffing Challenges | 4.6 |
| Training Challenges | 4.0 |

As the final step of this data collection, each expert was asked to rate the level of agreement with each theme on the same scale as presented in Round 2. The same measurement of central tendency was utilized to test areas of consensus, with those achieving a mean score of 4 or higher indicating consensus and those with a score of less than 4 as failing. The results of this analysis are included in Table 6.

Table 6
*Average expert score indicating consensus- All themes Round 3*

| **Identified Barriers** | **Average Expert Score (Scale of 1-5)** |
|---|---|
| Theme One | 4.7 |
| Theme Two | 4.9 |
| Theme Three | 4.0 |
| Theme Four | 4.9 |

A summary of findings is given below. Each of the themes presented to the experts achieved the measurement of consensus and were included in the development of the COPS model for cyber defense, presented in Chapter Five.

## Summary of Findings

This Delphi study has found four themes that contribute to the vulnerability of state and local law enforcement agencies in the U.S., particularly during times of civil unrest, according to law enforcement technology experts. Findings of this research found that department administrative controls, policies, and procedures can have a significant impact on controlling the likelihood of a hacktivist attack on an agency and on preparing an agency to respond to and mitigate an attack, should one occur. Experts reached consensus on the following themes: police forces must actively manage the message and public perception during controversial law enforcement incidents; focus security efforts on critical or sensitive public-facing systems first; advocate, investigate, pursue, arrest and prosecute relevant to cybercrime; and misappropriation of time, money, skills, people, and processes pose the most significant defensive challenges for police forces to defend against cyber-attacks.

## Conclusion

Each iterative round of this qualitative Delphi study led to the identification of themes emerging from the responses of the identified state and local law enforcement technology experts. At the completion of the study, four themes were identified as reaching consensus among the panel. The themes achieving consensus focused on the contributing factors, systems of concern, the role of deterrence through arrest and prosecution as well as challenges faced by law enforcement agencies in defending against hacktivist cyber-attacks. From the themes achieving consensus and associated recommendations regarding defensive or mitigation tactics suggested by the experts, a model has been developed, which is presented in Chapter Five.

The four themes found in this study were compared to the previous literature for similarities and differences and were employed in the development of the COPS model for proactive cyber defense, which is detailed in Chapter Five.  The COPS model is responsive to the research question, fulfills the need for the study and may be readily implemented by thousands of law enforcement agencies across the U.S.

# CHAPTER 5. DISCUSSION, IMPLICATIONS, AND RECOMMENDATIONS

## Introduction

The U.S. was founded on the principles of individual liberty and the ability to protest injustices, perceived or real, even if the offending party is the government (Friedman, 2005). Since the foundation of the U.S., the country has been challenged with how to protect individual rights to protest injustices while still maintaining public safety and order (Maier, 1970). The enforcement arm of the executive branch was established under the Constitution, but the role of maintaining public order in civil disturbances has routinely fallen to the various law enforcement agencies serving state and local jurisdictions across the country (Andrews & Gaby, 2015; Smith A., 2017). For example, the role of the police in civil disturbances started with the Civil War, when the country was engaged in a struggle over the rights of to an entire race of people (LeGrande, 1968). The Civil War presented citizens of the United States with a unique challenge: stand with the government and its representatives (the police) or stand against the government and fight (Smith W., 2012). The decision to stand up against the government led to the creation of the term *civil disobedience* (Thoreau, 1849).

Incidents of civil disobedience have occurred several times in history when United States citizens perceived injustice (Friedman, 2005). In many cases, disobedience of authority was not only justified, but considered to be a solemn duty of citizens in a democratic society (Carson, Lapsanskey-Werner, & Nash, 2007; Linder, 2007). As the representatives of the government, law enforcement has been routinely called upon to respond to incidents of civil unrest associated with acts of civil disobedience and, as a result, has frequently become the most visible element of the government, especially when actions turn violent (Smith W., 2012).

As the U.S. has modernized and embraced the information age, law enforcement has gone through several phases of development, adopting new technologies at each stage to aid in responding more efficiently and safer than ever before to incidents involving civil unrest (Byrne & Marx, 2011; Newcombe, 2014). With IT modernization, there is an increased dependency on technology to respond (PERF, 2012; Office of Community Oriented Policing Services, 2015; Silberglitt et al., 2015). Recent incidents of civil unrest have taken advantage of technological innovation, leading to a new form of protest known as electronic civil disobedience, giving the protesters more capabilities to disrupt and posing new challenges to law enforcement agencies in the process (Bergal, 2017; Bonilla & Rosa, 2015; Cammaerts, 2015; Wray, 1999). Along with the United States, law enforcement technology evolution is paced by the equally rapid evolution of civil disobedience through the embrace of technology, which can lead to electronic civil disobedience at the hands and technical prowess of hackers (Sauter, 2014a).

Some hackers promote group causes and are termed hacktivist groups (McCormick, 2013). Since 2010, the U.S. has seen an increase in several hacktivist groups focused on hacking for a political or social cause (Coleman, 2014). The targeting of law enforcement systems is the modern evolution of civil disobedience. However, when combined with a growing dependency on technology by law enforcement agencies creates a significant technological business problem (Bergal, 2017).

This study included exhaustive research of existing literature on the theories of civil disobedience, the application of deterrence to hacking, and the culture of hacking as well as technology adoption and dependency within law enforcement. The literature review detailed in Chapter Two revealed a significant gap in the existing body of knowledge about hacktivism and electronic civil disobedience as well as recent studies surrounding law enforcement use of technology. Chapter Five presents the findings and compares the themes and emerging models against the existing literature for similarities and differences, and reports the model's implications for IT.

## Evaluation of Research Question

> RQ: What better model of cyber security defensive tactics could be developed to prepare U.S., state, and local law enforcement agencies to defend against hacktivist cyber-attacks in the future, as perceived by United States, state, and local law enforcement technology experts?

Answering the research question required identifying a model of cyber security defensive tactics that can be employed by the U.S., state, and local law enforcement agencies. Important themes surrounding challenges in cybersecurity and defensive tactics were identified in a multi-round interview of state and local law enforcement technology experts, whose responses informed the final themes and the basis of a new model. Each significant theme proposed defensive tactics; a brief discussion of the relationship to the existing literature for each theme is detailed below.

### Theme One: United States law Enforcement agencies should actively manage the message and public perception surrounding controversial law enforcement incidents

All of the experts participating in the research identified the first theme as significant. The theme suggests that law enforcement agencies should actively work to manage the message given to the media in an attempt to guide public sentiment and perception before, during, and following controversial or high-profile incidents to reduce the likelihood of the agency being targeted by hacktivists.

The idea that message management is a significant determinant in the success of actions associated with incidents of civil disobedience maps well to the concept of *signaling* and *sweet spot* protests as found in the literature, and is not a new theme (Glaser & Sunstein, 2016). The implication of actively managing information and public perception around incidents likely to spark civil unrest contributes to the proper application of deterrence through the disruption of communication, consistent with the theories on both deterrence and social movements (Freedman, 2004; Soderberg, 2013).

As noted by Soderberg (2013), hackers are often drawn to social movements, such as hacktivism campaigns, because of a perceived connection with a broader social cause and a shared struggle known as *collective action framing*. The ability of police agencies to counter-act the message driving a social movement and potentially draw hacktivists away from attacking police agencies is a key, non-technical component of successful cyber defense. While Beyer (2014) notes a current gap in the literature regarding the application of social movement theory to internet-based social actions, the existing comparisons to the physical world support the theme of taking an active role in the messaging surrounding a potentially controversial incident as a method of defense. History has proven that the absence or dismantling of an emotional or otherwise moving narrative can deal a significant blow to an activist movement, even online (Andrews & Gaby, 2015; Wanzo, 2015; Wray, 1999).

Theme One and the associated concept of *signaling* suggests that police be measured in response to incidents of civil unrest to avoid drawing broad rejection while being effective in maintaining or restoring public order, particularly when facing the challenge of dealing with non-violent protesters, i.e., the *sweet spot* of response (Glaser & Sunstein, 2016; Chenoweth & Stephan, 2011). One significant contributing factor to the success of online protests is the perception of online civil disobedience as non-violent and without lasting consequences. When faced with the perception of online protests being non-violent and limited in damage, the research by Chenoweth and Stephan (2011) found that law enforcement faces a distinct disadvantage when responding with any force (legal, technological, or otherwise) without seeming heavy-handed and possibly causing a public backlash against the police. The management of public perception, as suggested by Theme One, can serve as a potential mitigation technique by allowing police to detail the impacts of cyber-attacks on public safety and officer safety and, in the process, shifting the *sweet spot* of both the hacktivist and police actions, as defined by Glaser and Sunstein (2016).

Although the literature review identified the primary motivations behind hacktivist actions and the role of a deterrence declaration in preventing such an attack in the first place, existing literature fails to identify the practical step, identified in Theme One, that agencies may take to efficiently deter hacktivist actions (Goodman, 2010; Spafford, 2007). Because of the groundbreaking nature of this research, existing studies fail to recognize the connection between longstanding tactics and the application of theory to both physical protests and those that occur online. Existing literature neither explicitly agrees or disagrees with the first finding of this study. A constructive review of the literature around the application of theories to physical protests does demonstrate some support for the first theme, as identified by the experts in this research.

### Theme Two: United States law enforcement agencies should focus security efforts on critical or sensitive public-facing systems first

In Round One, seven of ten experts identified Theme Two: law enforcement agencies should make critical or sensitive public-facing systems the primary focus for any defensive tactics. The theme, directing the focus of agency defensive efforts, suggests that *public-facing* or internet-accessible public safety applications, as well as those most critical to agency operations, are the most likely to be targeted in the event of a hacktivist attack on a law enforcement agency and should be the primary focus of agencies' defensive efforts.

The existing literature failed to identify the particular characteristics of law enforcement systems that may be vulnerable to hacktivist attacks, leaving a significant gap in the current body of knowledge. Law enforcement leaders who may consider exposing systems to the internet because of its relative ease of implementation may be unaware of the potential threats introduced by that decision (Amoroso, 2016; Brooks, 2014).

As found in the literature review, four of ten experts specifically identified the risks associated with the targeting of public safety communications systems in Round One, with the theme gaining majority consensus among experts in Round 2. Public safety communications systems are of vital importance to law enforcement and the public served (Chan, 2001; Greenguard, Mullich, & Parch, 2016; Silberglitt, et al., 2015; Hawkins, 2013) but, as identified by the expert panel, are frequently overlooked as potentially vulnerable to cyber-attacks (Amoroso, 2016). While agencies in various stages of cybersecurity maturity routinely recognize that there is much work to be done in shoring up defenses, many may wonder where to begin (Amoroso, 2016). As with Theme One, the literature reviewed related to Theme Two contains significant gaps in failing to identify specific, practical actions that may be employed by agencies. The current literature did not provide any real solution and only identified the problem.

### Theme Three: United States law enforcement agencies should advocate for an increase in the investigation, pursuit, arrest, and prosecution of cyber threat actors as a method of deterrence

Theme Three suggested that law enforcement agencies should take an active role in working to increase the successful investigation, pursuit, arrest, and prosecution of hackers involved in criminal acts as a method of deterrence against hacktivists launching attacks against law enforcement agencies in the U.S. In Round One, five of the ten experts identified the successful arrest and prosecution of cyber threat actors as a potential deterrent in curbing cyber-attacks against law enforcement agencies. Theme Three gained majority consensus in Round 2 and was later confirmed in Round 3, with only one expert dissenting and expressing concern over the reality of capturing anonymous or foreign actors, a concern aligned with one source found in the literature (Denning, 2015).

As a preemptive method of deterrence, the proactive approach of to deter cybercrime through increased efforts to find and punish illegal hackers is similar to the findings of Freedman (2004) that the threat of law currently on the books does little to deter a potential cyber threat actor unless a real threat of being caught exists. The second requirement for effective criminal deterrence is credibility and communication (Kennedy, 1983), which constitutes a method of preemptive deterrence (Freedman, 2004).

The use of preemptive deterrence methods to reduce the frequency and effectiveness of cyber-attacks is an idea supported by the official guidance provided by the National Institutes of Justice (2016). The National Institutes of Justice (2016) noted in a publication that law enforcement could deter criminal activity by merely increasing the perception that criminals will be caught and punished. In the event of a criminal cyber-attack against a law enforcement agency, the police are positioned in a unique role as both investigator and victim (Bergal, 2017).

The dual role of investigator and victim positions law enforcement agencies not only to pursue cybercriminals more aggressively, but also to take a stronger cybersecurity role in increasing evidence collection, which is likely to lead to a more successful prosecution in the event the hacker can be identified (Smith W., 2012).

Additional support for the approach of using an increase in the threat of being caught for cybercrime through the increased investigation and prosecution of criminal hackers as a defensive method is supported by Hobbes and Gaskin (1998), who outlined the individual human effect of deterrence in detail. According to Hobbes and Gaskin (1998), an individual will pursue self-interests as long as the value proposition remains in favor of the one deciding to take action. Consistent with the theme of police working to increase the likelihood of hackers getting caught and sent to jail is a tactic with the goal of shifting the value proposition of hacking, mainly when targeting law enforcement agencies.

The current literature surrounding deterrence theory documents the concept of deterrence by denial (Goodman, 2010). Approaches to denial include a reduction in capability, communication, and credibility (Goodman, 2010). The reduction in each category may be accomplished as suggested by the experts, suggesting that the suggestions on deterrence made by Goodman (2010) and Freedman (2004) that through an increase in the arrest and prosecution of cybercriminals a more compelling deterrent declaration is made to other potential cyber threat actors still holds true today.

Consistent with the concern expressed by the single dissenting expert, a few articles suggest that the application of deterrence theory in cybersecurity is more complicated (Geers, 2010). According to Geers (2010) and Denning (2015), the complications are mainly because of the malleability of cyberspace, the ability to operate online anonymously and more directly related to this theme, which is the international nature of many cybercrimes. While the first two complications listed will be overcome only through advances in investigatory technology and time, the third complication of applying deterrence theory to cybersecurity can be overcome through actions suggested in Theme Three and in better partnerships between the U.S. and international law enforcement authorities.

### Theme Four: United States law enforcement agencies should focus on optimization of time, money, skills, people, and processes to overcome the most significant defensive challenges

Theme Four suggested that a lack of optimization in time management, budget allocation, skill development, personnel allocations, and process refinement related to cyber defense represent the most significant barriers to effective agency cyber defense, according to the expert panel. The barriers of time, money, skills, people, and processes were each identified in Round One by six, four, four, six, and five of ten experts, respectively. When presented to the experts in Round 2, each barrier gained majority consensus, which was later confirmed in Round 3.

Law enforcement agencies face internal and external challenges to efficiently defending technology assets from the threat of a cyber-attack (Bergal, 2017), (FBI, 2015). While the concept of investing time, personnel, and money in cybersecurity defense is not a new theme, highlighting the importance of administrative investments to successful cyber defense will prompt administrators to understand and respond better to the non-technical nature of cybersecurity (Amoroso, 2016).

The importance that a skilled cybersecurity workforce plays in defending law enforcement agencies was officially acknowledged in a 2015 speech by then FBI director James Comey (as cited in Peterson, 2015) who said, “I have to hire a great workforce to compete with those cybercriminals, and some of those kids want to smoke weed on the way to the interview” (para. 14). Director Comey identified a key challenge facing law enforcement and other government agencies alike: the balance between traditional values and regulatory controls and attracting the best and brightest talent in cybersecurity (Smith G, 2017). Traditionally, law enforcement and government agencies have not hired individuals with any criminal past or recent drug use, both of which can be incompatible with many individuals either currently or previously a part of the hacker culture. However, those individuals often possess the most desirable skills (Peterson, 2015; Smith G, 2017).

The challenge of overcoming hiring challenges presented by traditional standards leaves law enforcement agencies at a crossroads when attempting to hire skilled cybersecurity workers: either relax hiring standards to compete for those with skills but a blemished past, or remain steadfast in standards, taking those with both skills and a clean past while training others and working to retain both (Peterson, 2015; Collett, 2016). Both approaches are supported by Theme Four, which focuses broadly on creating an organizational approach to cybersecurity that places appropriate value on people, processes, and training.

Theme Four presents an actionable path forward, which fills a gap in the current literature and can be adopted by law enforcement executives in supporting their cybersecurity professionals and better preparing for a future cyber-attack. No literature reviewed directly conflicts with the idea presented by the experts in Theme Four and, while additional literature exists regarding cybersecurity recruitment and retention, none relates directly to law enforcement agencies and the impact that this theme may have in increasing cyber defense, making this theme an entirely new finding.

## Fulfillment of Research Purpose

The fulfillment of the research purpose resulted in four themes, which are entirely new in the approach to defending law enforcement agencies against the modern threat of cyber-attacks, particularly when perpetrated by hacktivists. While the existing literature overwhelmingly supports the underlying principles contained in the themes identified, the existing research has a gap in the body of knowledge when applying defensive tactics to the unique challenges posed by hacktivists attacks on law enforcement agencies.

The outcome of this research and the themes developed from the consensus of the expert panel is the proactive cyber defense model of Control, Organize, Pursue, and Staff (COPS). When implemented, the COPS model will empower law enforcement executives in the U.S. to protect the systems vital to their services delivery from the impacts of hacktivism much earlier in the cyber kill-chain than governance or controls contained in other cybersecurity frameworks and standards. The unique contribution of the COPS model to the law enforcement and research communities, when compared against earlier, more comprehensive cybersecurity frameworks, such as the ISO 27000 series and the NIST Cybersecurity Framework, is that the elements of the COPS model are primarily focused on prevention and guiding a department's response to the threat of an attack. The key differentiator of the COPS model, when compared to the ISO and NIST publications, is the focus on disruption of the attack before the first phases of the cyber-attack occur, making the COPS model entirely new and incomparable but complementary to existing cybersecurity models. The COPS model also overcomes some of the criticisms found in the literature of the existing cybersecurity frameworks because it provides an open, industry-specific model complete with actionable steps that agencies can take to reduce overall cybersecurity risk.

Law enforcement IT systems are not only critical to agency operations but are equally critical to the security and safety of society as a whole. Disruption of crucial public safety systems when law enforcement is attempting to maintain public order is of particular concern, where the likelihood of significant loss of life or property is very high.

## Elements of the COPS model

### Control the message

Control is responsive to Theme One as identified by the experts; law enforcement agencies should actively work to manage the message portrayed to the media in an attempt to guide public sentiment/perception before, during, and following controversial or high-profile incidents. The first point of the COPS model, *control the message*, focuses on methods that police can use as a preemptive deterrent against hacktivist movements. Law enforcement agencies should engage with the public with openness and transparency when possible, taking into consideration the potential cyber impacts following a controversial law enforcement incident that may attract the attention of civil activists and hacktivists.

The control element of the COPS model affords law enforcement leaders the opportunity to implement defensive tactics proactively to potentially deter a hacktivist attack from occurring or at least mitigate its impact. While the theme of law enforcement taking an active role in keeping the media and public informed is far from new within the broader scope of criminal justice administration, the role public relations plays relative to cybersecurity, mainly as a defensive tactic, is unique to the COPS model. Agencies may struggle to obtain funding or the expertise to combat cyber threats from a technical standpoint. The control element of the COPS model reveals a low-cost defensive measure that requires slight modifications in the way an agency faces public relations following a high-profile incident.

Particular attention should be paid when attempting to control public sentiment around controversial events on ensuring such a plan is exercised and employed when agencies face a politically or socially charged incident. IT and security components should offer assistance to the agency to promote transparency and proactive information dissemination where possible.

Relationships (both formal and informal) should also be established with service providers, to include internet service providers, intelligence centers (such as state and local fusion centers), and media outlets ahead of incidents. Building productive relationships with service providers will allow police to leverage pre-established partnerships when responding to a hacktivist incident.

Finally, the control element is responsive to Theme Two in that *public-facing* or internet-accessible public safety applications and those most critical to agency operations are most likely to be targeted in the event of a hacktivist attack on a law enforcement agency and should be the primary focus of agencies' defensive efforts. As a part of the control element, agencies should continue preparatory technical efforts on tuning firewalls and other security technologies to respond quickly to an attack and preparing end-users for social engineering techniques through proper security awareness training.

**Organize systems according to their classification**

Responsive to Theme Two identified by the experts, *public-facing* or internet-accessible public safety applications and those most critical to agency operations are most likely to be targeted in the event of a hacktivist attack on a law enforcement agency and should be the primary focus of agencies' defensive efforts. As a method of defense in response to Theme Two from the research, the organizing element of the COPS model includes the action that agencies should limit public-facing (internet-accessible) critical applications and servers wherever possible. When impossible to eliminate public exposure, the defensive focus should shift to advanced techniques, such as stronger authentication, access control policies, and encryption (both in-transit and at rest).

Responsive to Themes Two and Four regarding the protection of critical systems and investing in the education of employees, agencies should work to eliminate gaps in security found in public safety communications and other critically sensitive systems through the education of non-IT communications technicians and vendors as well as a renewed focus on security engineering of communication systems. The renewed focus on security engineering can be implemented through system design reviews, vulnerability assessments, and system hardening.

**Pursue resources, policies, and legal avenues to increase the likelihood of arrest and prosecution of cybercriminals**

The pursue element of the COPS model is responsive to Theme Three, as identified by the experts, which notes that law enforcement agencies should take an active role in increasing the successful investigation, pursuit, arrest, and prosecution of hackers. The pursue element of the COPS model proposes that police should advocate for stronger laws, increased resources, and better evidence preservation to increase the likelihood of the successful arrest and prosecution of cybercriminals. Agencies can employ the COPS model not only to have a positive impact on its proactive cyber defense but also to make a broader impact on our communities and nation.

The action *pursue* presents an entirely new defensive approach through preemptive deterrence, which has either not been considered or may seem out of reach for many agencies due to legal restrictions and lack of dedicated resources. With the broad implementation of the model proposed, law enforcement agencies can collectively affect change in the investigation and prosecution of cybercriminals. Law enforcement should contribute to cyber deterrence through the increased arrest and prosecution of cyber actors, and law enforcement should advocate for an update and strengthening of cybercrime laws. Legislative actions must focus on penalties but also the requirement for victims to report criminal actions.

Agencies should also work to dedicate attention and resources to the investigation and pursuit of cybercriminals. Included in the implementation of this model is the education for judges and prosecutors on digital investigations and evidence. Where possible, agencies should limit inbound network traffic to U.S.-based entities through IP address filtering and geo-fencing techniques to increase the likelihood of successful prosecution in the event of an attack against law enforcement systems. For example, by limiting access to a sensitive law enforcement application to devices located in the United States, prosecution is potentially easier due to the applicability of U.S. law and the ability for law enforcement to apprehend the hacker in the event of an attack.

### Staff cybersecurity with the personnel, budget, training, and refined processes necessary to mount a formidable cyber-defensive capability

The final element of the COPS model, Staff, is responsive to the fourth theme, identified by the experts as a lack of optimization in time management, budget allocation, skill development, personnel allocations, and process refinement that represents the most significant barriers to effective agency cybersecurity no additional rounds were required. The staff element of the COPS model proposes that agencies should work to educate stakeholders to include executives and human resources on cyber threats and defensive challenges. Educating stakeholders will encourage top-level buy-in to the cybersecurity strategy, opening up opportunities for funding and personnel allocations.

Law enforcement agencies should focus initial defensive efforts on non-technical solutions to include optimization of time, training, budget, personnel allocations related to cyber defense. Many of the investments in cybersecurity are neither technical or expensive but instead administrative. Agencies as a whole should leverage in-house, virtual, and partner-provided training to educate staff efficiently and establish partnerships with local schools and colleges to encourage careers in cybersecurity, particularly within law enforcement agencies.

Executives can change the organizational culture to view cybersecurity as an on-going operational expense rather than a one-time capital (equipment) expense, and advocate for industry training standards and stricter penalties for non-compliance with cybersecurity policies. For example, executives should focus on the integration of cyber intelligence into the agency's defensive strategy through leading efforts to establish partnerships with existing cyber intelligence sources and an internal plan to consume and act upon intelligence gathered. By focusing attention on the areas of security deemed most relevant through the use of intelligence, agencies can focus limited resources and training on those threats most likely to impact the agency in the near term, reducing strain on existing personnel and technologies.

## Contribution to Business Technical Problem

The general problem addressed by this study is that the combination of law enforcement's growing dependency on technology and the increasing threat posed by hacktivism has created a potential crisis, leaving state and local law enforcement response capabilities in a vulnerable state (Bergal, 2017; Amoroso, 2016; Lum, Koper, & Willis, 2016). Events of civil disobedience witnessed from as early as 2010 through the present day are changing the nature, identity, and effectiveness of hacktivism to disrupt technologies critical to state and local law enforcement operations (Coleman, 2014). The specific problem is that the effectiveness by hacktivists and the growing dependency on technology by state and local law enforcement has created a more significant attack surface that agencies are increasingly unprepared to protect (Newcome, 2015).

This research directly contributes to the cyber defense of state and local law enforcement agencies in the U.S. The COPS model represents a holistic framework of proactive actions that law enforcement agencies can take to provide better protection against the actions of hacktivists or other cyber threat actors. The model focuses primarily on simple, low-tech actions that all agencies can adopt to launch an effective defense, regardless of the current maturity of their cybersecurity posture. These actions are likely low cost. The findings presented in this research are previously undocumented in academic literature and contribute significantly to the body of knowledge regarding cybersecurity. The themes identified by the expert panel in this research were used to formulate the COPS model of proactive cybersecurity defensive tactics, making it one of the few if not exclusive data-driven models focused on law enforcement agency cyber defense.

## Recommendations for Further Research

The constant, rapid evolution of cybersecurity threats requires defensive tactics to be frequently updated. Future research should focus on expansion and update of the COPS model to account for new threats that were not addressed or could not have been foreseen during this research study. For example, this research could be expanded or modified to adjust the model for applicability to federal or foreign police agencies. Given additional resources and time, the field of experts could be broadened to develop a more expansive, yet simple, non-industry-specific defensive model, which is in dire need in light of recent data breaches across multiple industries and the complexity involved with the implementation of more complex frameworks, such as ISO27000 and the NIST National Cybersecurity Framework.

The variables discovered through this qualitative study could serve as the basis for a quantitative study based on data collected from law enforcement agencies regarding the themes presented in this research. For example, a quantitative study on the number of prosecutions resulting from cybercrimes compared to the number of cyber-attacks in the United States, when tracked over time, could determine the efficacy of prosecution as a deterrent to cybercrime. Another example for potential future research is testing the theme regarding protection of public-facing systems. By exploring data derived from data breach reports, a study could be conducted to determine if public-facing systems are more frequently attacked compared to those secured behind a firewall or on a private network and would be useful to substantiate the validity of this model.

## Conclusion

This qualitative Delphi study resulted in the development of a model consisting of defensive tactics that may be employed by law enforcement agencies in the United States to prepare better for defense against hacktivist attacks. The study consisted of a multi-round iterative series of interviews with law enforcement technology experts to gather a consensus of the expert perspectives surrounding appropriate defensive tactics. While individual responses varied slightly regarding the most efficient way to defend against hackers with a political or social motivation, the themes that gained consensus among experts identified factors contributing to attacks, vulnerable systems, and the role of deterrence in cyber defense. The themes that gained consensus among the experts were those that identified the barriers to agency defense and emerging technology challenges to law enforcement agencies. Each theme was examined and used to develop a model of defensive tactics that can be employed by law enforcement agencies to improve protection against the adverse effects of hacktivism.

The resulting model, COPS, provides specific guidance to agencies wishing to prepare better for incidents where hacktivists may target the systems vital to agency operations. While the current literature consists of significant gaps in cybersecurity defense. The literature does provide existing theories on the motivations behind cyber threat actors that must be studied in order to apply appropriate defensive controls. The COPS model both fill this gap in the literature and provide police agencies with a low-cost, actionable model to employ when attempting to defend sensitive systems and data against cyber-attacks.

Chapter Five represents the conclusion of this research. The potential impact of the study and the model contained therein is limited only by its adoption by the agencies it was designed to assist. The study is on the leading edge of an area in desperate need of additional research and focus by industry experts and scholars. Technology and cybersecurity hold enormous promise to solve massive societal and law enforcement problems now and, in the future (Amoroso, 2016). Only through a constant pursuit of knowledge and filling the gaps in global knowledge will the human race be free to explore, innovate and create to its fullest potential (Maughan, 2010).

## References

Accenture. (2016). *Optimizing policing for the future.* Accenture Consulting. Retrieved from https://www.accenture.com/_acnmedia/PDF-45/Accenture-Optimising-Policing.pdf

Amoroso, E. (2016, October). Cybersecurity: a call to action for police executives. *The Police Chief*, 28-33. Retrieved from http://www.policechiefmagazine.org/wp-content/uploads/PoliceChief_October_2016LORES1.pdf

Andrews, D. A., & Bonta, J. (2014). *The psychology of criminal conduct*. Routledge. Retrieved from https://www.taylorfrancis.com/books/9781317521501

Andrews, K., & Gaby, S. (2015, June). Local protest and federal policy: the impact of the civil rights movement on the 1964 Civil Rights Act. *Sociological Forum, 30*(S1), 509-527. doi:10.1111/socf.12175

Bejtlich, R. (2015). Strategic defense in cyberspace: beyond tools and tactics. In *Cyber War in Perspective: Russian Aggression against Ukrain*e (pp. 159-170). Tallinn: NATO CCD COE Publications. doi:10.1016/C2013-0-00059-X

Bergal, J. (2017, January). Hacktivists launch more cyberattacks against local, state governments. *PBS Stateline*. Retrieved from http://www.iacpcybercenter.org/news/hacktivists-launch-more-cyberattacks-against-local-state-governments/

Bevan, N., & Earthy, J. (2017). Benefiting from ISO standards. In K. L. Norman, & J. Kirakowski, *The Wiley Handbook of Human Computer Interaction.* John Wiley & Sons Ltd. doi: https://doi.org/10.1002/9781118976005.ch3

Beyer, J. L. (2014). The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate Party and Iceland. *Journal of Computer-Mediated Communication, 19*(2), 141-154.

Bonilla, Y., & Rosa, J. (2015). #Ferguson: digital protest, hashtag ethnography, and the racial politics of social media in the United States. *American Ethnologist, 00*(0), 4-16. Retrieved from http://blogs.umass.edu/jdrosa/files/2015/01/Bonilla-Rosa-2015-Ferguson.pdf

Brandl, S. G. (2003). Back to the future: the implications of September 11, 2001 on law enforcement practice and policy. *Ohio State Journal of Criminal Law*, 133-154. Retrieved from http://hdl.handle.net/1811/72586

Brooks, A. (2014). *Law enforcement information management study.* Framingham, MA: IDC. Retrieved from https://cacp.ca/index.html?asst_id=977

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing: a review of the research on implementation and impact. *Journal of Police Studies, 20*(3), 17-40.

Cammaerts, B. (2015). Social media and activism. In R. Mansell, & P. Hwa, *The International Encyclopedia of Digital Communication and Society.* Oxford UK: The London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/62090/1/Social_media_and.pdf

Carson, C., Lapsanskey-Werner, E. J., & Nash, G. B. (2007). In *The Struggle for Freedom: A History of African Americans* (p. 206). New York, NY: Pearson Longman.

Cartwright, D. (2017, April 18). So, you're 'ISO 27001 accredited' huh? Just saying so doesn't cut it. *The Register*. Retrieved from https://www.theregister.co.uk/2017/04/18/protect_your_digital_enterprise_iso_27001_explainer/

Chan, J. (2001). The technological game: how information technology is transforming police practice. *Criminology and Criminal Justice, 1*(2), 139-159.

Chenoweth, E., & Stephan, M. J. (2011). *Why civil resistance works: the strategic logic of nonviolent conflict.* West Sussex, England: Columbia University Press.

Chia-Chien, H., & Sandford, B. A. (2007, August). The Delphi technique: making sense of consensus. *Practical Assessment, Research & Evaluation, 12*(10).

Christensen, S., Caelli, W. J., Duncan, W. D., & Georgiades, E. (2010, April 27). An Achilles heel: denial of service attacks on Australian critical information infrastructures. *Information & Communications Technology Law, 19*(1), 61-85. Retrieved from http://dx.doi.org/10.1080/13600831003708059

Cole, Z. D., Donohoe, H. M., & Stellefson, M. L. (2013, March). Internet-based Delphi research: case-based discussion. *Environ Manage*, 511-523. doi:10.1007/s00267-012-0005-5

Coleman, G. (2014). Introduction: "And now you have got our attention." In *Hacker, Hoaxer, Whistleblower, Spy - The Many Faces of Anonymous* (pp. 1-18). Brooklyn, NY: Verso.

Collett, S. (2016, December 6). Hackers wanted: as its "bad guy" stereotype wanes, hacker job postings in the enterprise jump 700% in three years. *CSO Online*. Retrieved from https://www.csoonline.com/article/3145616/security/hackers-wanted.html

Cope, D. G. (2014, January). Methods and meanings: credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89-91. doi:10.1177/104973201129119299

Copeland, J. (2017). Implementing NIST CSF? Read this first. *Fair Institute*. Retrieved from https://www.fairinstitute.org/blog/implementing-nist-csf-read-this-first

Dabbagh, M., & Lee, S. P. (2014). An approach for integrating the prioritization of functional and nonfunctional requirements. *The Scientific World Journal*, 1-13. doi:10.1155/2014/737626

Dalal, R. S., & Gorab, A. K. (2016). Insider threat in cyber security: what the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In *Psychosocial Dynamics of Cyber Security* (1st ed.). New York, NY: Routledge. doi:10.4324/9781315796352-14

Deering, S., & Hinden, R. (2017). *Internet protocol, version 6 (IPv6) specification* (No. RFC 8200). Retrieved from: http://www.rfc-editor.org/rfc/pdfrfc/rfc8200.txt.pdf

Denning, D. (2015). Rethinking the cyber domain and deterrence. *Joint Force Quarterly, 77*(2), 8-15. Retrieved from http://hdl.handle.net/10945/45130

Dodge, C. (2016, March 17). The role of the institution on the adoption of law enforcement technology. *ISU ReD: Theses and Dissertations*. Normal, IL. Retrieved from https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=1494&context=etd

Federal Bureau of Investigation. (2009). *The FBI: a centennial history, 1908-2008.* Washington, DC: U.S. Department of Justice - Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/file-repository/fbi100book.pdf/view

Federal Bureau of Investigation. (2015). Hacktivists threaten to target law enforcement personnel and public officials. Federal Bureau of Investigation, U.S. Department of Justice.

Washington, DC: Internet Crimes Complaint Center. Retrieved from https://www.ic3.gov/media/2015/151118.aspx

Federal Communications Commission. (2016, February). *Narrow banding overview*. Retrieved from Federal Communications Commission: https://www.fcc.gov/general/narrowbanding-overview

First Responder Network Authority. (2016, July). *About First Net*. Retrieved from Firstnet.gov: http://www.firstnet.gov/about

Foley, B. J. (2010). Policing from the gut: anti-intellectualism in American criminal procedure. *Maryland Law Review, 69*(2). Retrieved from http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3420&context=mlr

Freedman, L. (2004). *Deterrence.* Cambridge, UK: Polity.

Friedman, L. (2005). *A history of American law.* (Touchstone, Ed.) New York, NY: Simon & Schuster.

Garlipp, M. (2015, June 18). Benefits of the NIST Cybersecurity Framework. *Gov Loop*. Retrieved from https://www.govloop.com/benefits-of-the-nist-cybersecurity-framework/

Gartner. (2017). *Top strategic predictions for 2018 and beyond: pace yourself, for sanity's sake.* Retrieved from https://www.gartner.com/doc/3803530?srcId=1-6595640685

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review, 26*, 298-303. Retrieved from https://s3.amazonaws.com/academia.edu.documents/46944723/j.clsr.2010.03.00320160701-4850-bapp3x.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1479608179&

Signature=vB6VSktIkxuRafW2t2VJch%2FyFNs%3D&response-content-disposition=inline%3B%20filename%3DThe_c

Glaser, E. L., & Sunstein, C. R. (2016, February). A theory of civil disobedience. *National Bureau of Economic Research Working Paper Series* (21338). Retrieved from http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein_851.pdf

Goodman, W. (2010). Cyber deterrence: tougher in theory than in practice? *Strategic Studies Quarterly*, 102-135. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a528033.pdf

Greenguard, S., Mullich, J., & Parch, L. A. (2016). *Next generation 911 for leaders in law enforcement.* (E. Reyes, D. Dytchkowskyj, & L. A. Parch, Eds.) Retrieved from 911.gov: http://www.911.gov/ng911_law/download/NG911_Resize_Mar2013_FINAL_LR.pdf

Harris, B., Konikoff, E., & Petersen, P. (2013). *Breaking the DDoS attack chain.* Carnegie Mellon University, Institute for Software Research, Pittsburg, PA. Retrieved from https://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf

Harris, F. (2015). The next civil rights movement? *Dissent, 63*(3), 35-40. Retrieved from https://franklinhslibrary.pbworks.com/w/file/fetch/101640115/Black%20Lives%20Matter.pdf

Hawkins, D. (2013). *Law enforcement tech guide for communications interoperability.* U.S. Department of Justice, Office of Community Oriented Policing Services. Washington DC: SEARCH Group, Inc. Retrieved from https://www.dhs.gov/sites/default/files/publications/cops-w0714-pub.pdf

Hobbes, T., & Gaskin, J. (1998). *Leviathan* (6th ed.). Oxford: Oxford University Press. Retrieved from https://content.taylorfrancis.com/books/download?dac=C2015-0-79410-3&isbn=9781315507606&format=googlePreviewPdf.

International Association of Chiefs Police. (2014). *IACP technology policy framework.* International Association of Chiefs of Police. Retrieved from http://www.theiacp.org/portals/0/documents/pdfs/iacp%20technology%20policy%20framework%20january%202014%20final.pdf

Infosec Institute. (2013, October 2). Hacktivism: means and motivations … what else? *Infosec General Security*. Retrieved from http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/#gref

Johnson, R. (2011). Anonymous occupation of Wall Street - here is what you missed. *Business Insider*. Retrieved from http://www.businessinsider.com/anonymous-occupy-wall-street-2011-9

Jordan, T. (2016). A genealogy of hacking. *Convergence: The International Journal of Research into New Media Technologies*, 1-17. doi:10.1177/1354856516640710

Jordan, T., & Taylor, P. (1998, November 1). A sociology of hackers. *The Sociological Review, 46*(4), 757-780. Retrieved from https://doi.org/10.1111/1467-954X.00139

Kennedy, K. C. (1983). A critical appraisal of criminal deterrence theory. *Michigan State University Faculty Publications*. Retrieved from https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1036&context=facpubs

Khadke, A., & Madankar, M. (2016, May). Implementation of DDoS attack preemption. *International Journal of Computer Applications, 141*(3), 7-11. Retrieved from https://pdfs.semanticscholar.org/94fe/8514662dd34239806a544d8134a1159ea46a.pdf

King, M. L. (1963). *Letter from Birmingham jail.* Retrieved from Aspen Institute: https://assets.aspeninstitute.org/content/uploads/files/content/docs/KING_LETTER_FROM_BIRMINGHAM_CITY_JAIL_(AS08).PDF

Koper, C. S., Lum, C., Willis, J., Woods, D., & Hibdon, J. (2015). *Realizing the potential of technology in policing.* George Mason University. Retrieved from http://cebcp.org/wp-content/technology/ImpactTechnologyFinalReport.pdf

Kurzman, C. (2003). The poststructuralist consensus in social movement theory. In J. Goodwin, & J. M. Jasper, *Rethinking social movements: structure, meaning, and emotion* (p. 111). Rowman & Littlefield Publishers.

LeGrande, J. (1968). Nonviolent civil disobedience and law enforcement policy. *Journal of Criminal Law and Criminology, 58*(3), 393-404. Retrieved from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5472&context=jclc

Li, X. (2013). Hacktivism and the first amendment: drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology, 27*(1), 302-329. Retrieved from http://jolt.law.harvard.edu/articles/pdf/v27/27HarvJLTech301.pdf

Linder, D. (2007). *The trial of Susan B. Anthony for illegal voting.* Retrieved from: http://law2.umkc.edu/faculty/projects/ftrials/anthony/sbaaccount.html

Lops, P., De Gemmis, M., Semeraro, G., Narducci, F., & Musto, C. (2011, October). Leveraging the LinkedIn social network data for extracting content-based user profiles. In *Proceedings of the fifth ACM conference on Recommender systems* (pp. 293-296). ACM. doi: 10.1145/2043932.2043986

Lum, C., Koper, C., & Willis, J. (2016). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly*. Retrieved from http://journals.sagepub.com/doi/pdf/10.1177/1098611116667279

Maier, P. (1970). Popular uprisings and civil authority in eighteenth-century America. *William and Mary Quarterly, 27*(1), 3-35. Retrieved from http://academic.csuohio.edu/humphreyt/History601/601%20Readings/Maier.pdf

Manadhata, P. K., & Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, (3), 371-386. doi: http://doi.ieeecomputersociety.org/10.1109/TSE.2010.60

Maughan, D. (2010, February). The need for a national cybersecurity research and development agenda. *Communications of the ACM, 53*(2), 29-31. doi:10.1145/1646353.1646365

McConnell, M. (2010, February 28). Mike McConnell on how to win the cyberwar we're losing. *The Washington Post*. Retrieved from http://www.cyberdialogue.ca/wp-content/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf

McCormick, T. (2013, April 29). Hacktivism: a short history. *Foreign Policy.* Retrieved February 14, 2016, fromhttp://foreignpolicy.com/2013/04/29/hactivisim-a-short-history/

McDowell, M. (2013, February 6). *Understanding denial-of-service attacks.* Retrieved from DHS US-CERT: https://www.us-cert.gov/ncas/tips/ST04-015

Mikhaylova, G. (2014). *The "Anonymous" Movement: hacktivism as an emerging form of political participation.* Texas State University. Retrieved from https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1

Moraetes, G. (2018). Choosing the Right Security Framework to Fit Your Business. *Security Intelligence*. Retrieved from https://securityintelligence.com/choosing-the-right-security-framework-to-fit-your-business/

Nadella, S. (2017). Annual Report 2017 (Rep.). Redmond, WA: Microsoft Corporation. Retrieved from https://www.microsoft.com/investor/reports/ar17/index.html

National Institute of Justice. (1998). *The evolution and development of police technology.* National Institute of Justice, The National Committee on Criminal Justice Technology. Washington DC: Seaskate, Inc. Retrieved from https://www.ncjrs.gov/pdffiles1/Digitization/173179NCJRS.pdf

National Institute of Justice. (2016). *Five things about deterrence.* Office of Justice Programs, U.S. Department of Justice. Washington, DC: National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/247350.pdf

Digitization/173179NCJRS.pdf

National Institute of Justice. (2016). *Five things about deterrence.* Office of Justice Programs, U.S. Department of Justice. Washington, DC: National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/247350.pdf

Newcombe, T. (2014). Forecasting the future for technology and policing. *Government Technology: Justice and Public Safety*. Retrieved from http://www.govtech.com/public-safety/Forecasting-the-Future-for-Technology-and-Policing.html

Newcome, T. (2015, November 3). Are states slacking on cybersecurity? *Government Technology: Security*. Retrieved from http://www.govtech.com/security/Are-States-Slacking-on-Cybersecurity.html

NIST. (2018a). *New to Framework*. Retrieved from NIST Cybersecurity Framework: https://www.nist.gov/cyberframework/new-framework#background

NIST. (2018b). *Uses and Benefits of the Framework*. Retrieved from NIST Cybersecurity Framework: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

Office of Community Oriented Policing Services. (2015). *The President's task force on 21st century policing implementation.* Washington, DC: The President's Task Force on 21st Century Policing Implementation. Retrieved from https://ric-zai-inc.com/Publications/cops-p341-pub.pdf

Oxford Dictionary. (2016). *British & World English dictionary*. Retrieved from Oxford Dictionary: http://www.oxforddictionaries.com/us/definition/english/hacktivist

Palacios, K. E., & Peterson, K. E. (2015). An Overview of Security Risk Management Concepts. In *Security Supervision and Management* (pp. 535-548). doi: https://doi.org/10.1016/B978-0-12-800113-4.00040-7

Pemberton, C. (2017, January 1). *Gartner predicts 2017: marketers, expect the unexpected.* Retrieved from Gartner Reports: https://www.gartner.com/smarterwithgartner/gartner-predicts-2017-marketers-expect-the-unexpected/

Police Executive Research Forum. (2012). *How are innovations in technology transforming policing?* Washington, DC: Police Executive Research Forum. Retrieved from http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf

Peterson, A. (2015, October 24). How the government tries to recruit hackers on their own turf. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/10/24/how-the-government-tries-to-recruit-hackers-on-their-own-turf/?utm_term=.beb697a9818e

Pew Research Center. (2018). *Mobile fact sheet.* Pew Research Center. Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

Phillips, R. (2000). New applications for the Delphi technique. *Annual "San Diego" Pfeiffer and Company, 2*, 191-196.

Ponemon Institute. (2017). *2017 cost of cybercrime study.* Ponemon Institute. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Quackenbush, S. L., & Zagare, F. C. (2016, May). Modern deterrence theory: research trends, policy debates, and methodological controversies. *Oxford Handbooks Online*. doi:10.1093/oxfordhb/9780199935307.013.39

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R., Saraf, P.,... & Kuhlman, C. (2014, August). 'Beating the news' with EMBERS: forecasting civil unrest using open source indicators. In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 1799-1808). ACM. doi: 10.1145/2623330.2623373

RAND Corporation. (2016). *Delphi Method*. Retrieved from RAND Corporation: www.rand.org/topics/delphi-method.html

Rawls, J. (1971). *A theory of justice.* Cambridge, MA: Harvard University Press. Retrieved from http://www.csus.edu/indiv/c/chalmersk/econ184sp09/johnrawls.pdf

Rogers, A. (2014). What Anonymous is doing in Ferguson. *Time*. Retrieved from http://time.com/3148925/ferguson-michael-brown-anonymous/

Rothrock, R., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15. Retrieved from https://search.proquest.com/openview/07e2904086d30255ee3c570a6aee0196/1?pq-origsite=gscholar&cbl=26142

Rukh, L., & Malik, A. A. (2017). Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management. *2017 International Conference on Communication Technologies (ComTech).* Rawalpindi, Pakistan: IEEE. doi:10.1109/COMTECH.2017.8065742

Sauter, M. (2013). *Distributed denial of service actions and the challenge of civil disobedience on the internet.* Cambridge, MA: Massachusetts Institute of Technology. Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/81079/857841575-MIT.pdf?sequence=2

Sauter, M. (2014a). Blockades and blockages: DDoS as direct action. In *The Coming Swarm* (pp. 39-59). New York, NY: Bloomsbury Academic.

Sauter, M. (2014b). DDoS and civil disobedience in historical context. In *The Coming Swarm* (pp. 19-36). New York, NY: Bloomsbury Academic.

Shackleford, S., Proia, A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal, 50*(2-3), 305-356. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/tilj50&i=333.

Siff, S. (2016, May). Policing the police: a civil rights story. *Origins, 9*(8). Retrieved from http://origins.osu.edu/article/policing-police-civil-rights-story

Silberglitt, R., Chow, B. G., Hollywood, J. S., Woods, D., Zaydman, M., & Jackson, B. A. (2015). *Visions of law enforcement technology in the period 2024-2034.* Police Executive

Research Forum. Santa Monica, CA: RAND Corporation. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/248718.pdf

Simmons, K. C. (2015, November 18). Police technology shouldn't replace community resources. *The New York Times*. Retrieved from https://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/police-technology-shouldnt-replace-community-resources

Smith, A. (2017). Record shares of Americans now own smartphones, have home broadband. Pew Research Center. Retrieved from http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

Smith, G. (2017, December 06). Feds turn to hackers to defend nation in cyberspace. *Huffington Post*. Retrieved from https://www.huffingtonpost.com/2011/08/08/government-recruits-hackers-cyber-shortage_n_920795.html

Smith, W. (2012). Policing civil disobedience. *Sage Journals-Political Studies, 60*(4), 826-842. Retrieved from http://journals.sagepub.com/doi/abs/10.1111/j.1467-9248.2011.00937.x

Smith, W. (2016). The burdens of conviction: Brownlee on civil disobedience. *Criminal Law and Philosophy, 10(4)*, 693-706. Retrieved from https://doi.org/10.1007/s11572-014-9336-z

Soderberg, J. (2013, January 13). Determining social change: the role of technological determinism in the collective action framing of hackers. *New Media Society*, 1277-1294. doi:10.1177/1461444812470093

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M., & Buyya, R. (2017). Combating DDoS attacks in the cloud: requirements, trends, and future directions. *EEE Cloud Computing, 4*(1), 22-32. doi:10.1109/MCC.2017.14

Spafford, E. H. (2007). Are computer hacker break-ins ethical? *Internet Security: Hacking, Counterhacking, and Society*, 49. Retrieved from http://csrc.nist.gov/publications/secpubs/tr994.pdf

Stanford University. (2013, December 20). *Civil disobedience*. Retrieved from Stanford Encyclopedia of Philosophy: http://plato.stanford.edu/entries/civil-disobedience/

Stanford University. (2016). *What is hacktivism?* Retrieved from Stanford Computer Science: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

Stevens-Henager College. (2013, April 29). *What is emerging technology?* Retrieved from https://www.stevenshenager.edu/blog/what-is-emerging-technology

Sutliff, U., & Richardson, T. (2016, June). Cybersecurity guide for state and local law enforcement. Washington, DC: National Consortium for Advanced Policing.

Thoreau, H. D. (1849). *Resistance to civil government.* Retrieved from Thoreau E-Server: http://thoreau.eserver.org/civil.html

Tilly, C., & Wood, L. J. (2015). Social Movements 1768-2012. Routledge. Retrieved from https://www.taylorfrancis.com/books/9781317251941

United States. Const. amend. I

United States. (1776). Declaration of Independence.

United States Council of Economic Advisors. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*. Executive Office of the President of the United States. Washington DC: Executive Office of the President of the United States. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicous-Cyber-Activity-to-the-U.S.-Economy.pdf

United States. Department of Justice. (2016, July 25). *Terms & definitions: law enforcement*. Retrieved from U.S. Department of Justice - Bureau of Justice Statistics: http://www.bjs.gov/index.cfm?ty=tdtp&tid=7

United States Bureau of Justice Statistics. (2011, July). *Census of state and local law enforcement agencies, 2008.* Retrieved from United States Bureau of Justice Statistics: http://www.bjs.gov/content/pub/pdf/csllea08.pdf

Wanzo, R. (2015). In *Suffering will not be televised: the African American women and sentimental political storytelling* (p. 29). SUNY Press.

Watson, V., Tellabi, A., Sassmannahausen, J., & Lou, X. (2017). Interoperability and Security Challenges of Industry 4.0. *INFORMATIK*, 973-985. doi:10.18420/in2017_100

Wood, C. (2015, August 28). Unmasking hacktivism and other high-profile cyberattacks. *Government Technology: Justice and Public Safety*. Retrieved from http://www.govtech.com/public-safety/Unmasking-Hacktivism.html

Wood, C. (2018, January 6). People want more police technology, but not more surveillance. *State Scoop*. Retrieved from http://statescoop.com/people-want-more-police-technology-but-not-more-surveillance

Workman, M., Phelps, D. C., & Gathegi, J. N. (2012). *Information security for managers.* Jones and Bartlett Publishers, Inc.

World Economic Forum. (2014). *Global risks 2014.* Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

World Economic Forum. (2018). *Global risks report.* World Economic Forum. Retrieved from http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/

Worrall, J. L., & Schmalleger, F. J. (2013). Origins and evolution of American policing. In *Policing.* PH Professional. Retrieved from http://www-fp.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/samplechapter/0133028313.pdf

Wray, S. (1999, March). On electronic civil disobedience. *Peace Review, 11*(1), 107-111. doi: http://dx.doi.org/10.1080/10402659908426237

Ziglio, E. (1996). The Delphi method and its contribution to decision-making. In M. Alder, & E. Ziglio, *Gazing Into The Oracle* (pp. 3-4). Jessica Kingsley Publishers.

## STATEMENT OF ORIGINAL WORK

### Academic Honesty Policy

Capella University's Academic Honesty Policy (3.01.01) holds learners accountable for the integrity of work they submit, which includes but is not limited to discussion postings, assignments, comprehensive exams, and the dissertation or capstone project.

Established in the Policy are the expectations for original work, rationale for the policy, definition of terms that pertain to academic honesty and original work, and disciplinary consequences of academic dishonesty. Also stated in the Policy is the expectation that learners will follow APA rules for citing another person's ideas or works.

The following standards for original work and definition of *plagiarism* are discussed in the Policy:

> Learners are expected to be the sole authors of their work and to acknowledge the authorship of others' work through proper citation and reference. Use of another person's ideas, including another learner's, without proper reference or citation constitutes plagiarism and academic dishonesty and is prohibited conduct. (p. 1)
>
> Plagiarism is one example of academic dishonesty. Plagiarism is presenting someone else's ideas or work as your own. Plagiarism also includes copying verbatim or rephrasing ideas without properly acknowledging the source by author, date, and publication medium. (p. 2)

Capella University's Research Misconduct Policy (3.03.06) holds learners accountable for research integrity. What constitutes research misconduct is discussed in the Policy:

> Research misconduct includes but is not limited to falsification, fabrication, plagiarism, misappropriation, or other practices that seriously deviate from those that are commonly accepted within the academic community for proposing, conducting, or reviewing research, or in reporting research results. (p. 1)

Learners failing to abide by these policies are subject to consequences, including but not limited to dismissal or revocation of the degree.

## Statement of Original Work and Signature

I have read, understood, and abided by Capella University's Academic Honesty Policy (3.01.01) and Research Misconduct Policy (3.03.06), including the Policy Statements, Rationale, and Definitions.

I attest that this dissertation or capstone project is my own work. Where I have used the ideas or words of others, I have paraphrased, summarized, or used direct quotes following the guidelines set forth in the APA *Publication Manual*.

Learner name
and date /s/ Patrick J. Woods 05/10/2018

Mentor name
and school Dr. Kimberly Lowrey, Capella University

## APPENDIX A

### Round 1 Questionnaire with Demographic Questions

Delphi Study – Patrick J. Woods, Capella University
Participant ID (to be completed by the researcher):

Q1. In your expert opinion are hacktivist attacks against law enforcement on the rise and/or likely to occur in the future? If so why?

Q2. What would be the primary factors contributing to hacktivist targeting law enforcement?

Q3. At a high level, what types of systems or department processes are most likely to be impacted by hacktivist attacks on a law enforcement agency?

Q4. What role (if any) does deterrence play in curbing attacks by hacktivists?

Q5. What are the most significant barriers (if any) facing law enforcement in protecting their IT systems?

Demographic questions

- Total years of experience in law enforcement
- Total years of experience with law enforcement technology
- Current Position
- Do you lead technology efforts for a State or Local Law Enforcement agency?
- Highest Level of Education Obtained

  - Major/Area of Concentration

- Do you have any experience in responding to an incident impacted by hacktivism?

- Do you have any experience in the creation, interpretation, or implementation of CJIS Security Policy?

  - Briefly, explain role

# APPENDIX B

## Round 2 Questionnaire

Delphi Study – Patrick J. Woods, Capella University
Round 2
Participant ID (to be completed by the researcher):

In Round 1, several themes began to emerge. It is from these themes that the questions presented below are developed. Additionally, you are given the opportunity to change your response in light of the consensus gained among other participants or further justify your position that may differ from others responding. Selection of focus areas for Round 2 was based on two primary considerations: The contribution of the topic toward answering the research question and level of initial consensus.
Q1. In Round 1, a considerable amount of focus was placed on the following areas as significant factors driving the targeting of law enforcement by hacktivists. Understanding that defensive tactics employed by law enforcement can be both technical and administrative in nature, please indicate on a scale of 1-5 (1 – Strongly disagree; 5 – Strongly Agree) regarding your level of agreement regarding this factor playing a significant role in influencing hacktivism targeting law enforcement agencies. Additionally, indicate what controls/defensive tactics (technical (technology, procedures, etc.), administrative (policy, planning, communication, etc.), both or none) agencies could employ to better position their agencies (specifically IT components) to mitigate the likelihood that these factors will increase the probability of being attacked or the damage caused in the event of an active attack. Feel free to elaborate on specific tactics/changes/controls that you believe would be most effective.

A. Media Coverage/Public Sentiment 1-5:
    a. Potential Controls:
        i. Administrative
        ii. Technical
        iii. Both
        iv. Neither
    b. Specific tactics/changes/controls you believe would be most effective:

B. Reaction to controversial incidents 1-5:
    a. Potential Controls:
        i. Administrative
        ii. Technical
        iii. Both
        iv. Neither

b. Specific tactics/changes/controls you believe would be most effective:

C. Lack of cyber preparedness/ Agencies viewed as an easy target 1-5:
   a. Potential Controls:
      i. Administrative
      ii. Technical
      iii. Both
      iv. Neither
   b. Specific tactics/changes/controls you believe would be most effective:

Q2. Consensus existed in Round 1 surrounding each of the systems presented below as being those most likely to be impacted in the event of a hacktivist attack/movement against an agency. As in Question 1 above, please indicate your level of agreement on a scale of 1-5 that these systems would be primary targets for hacktivists. Additionally, please explain defensive tactics that could be employed to mitigate the potential impacts to each system and department operations.

A. Public-Facing Systems (Websites, email, web servers, etc.). 1-5:
   a. Potential defensive tactics:

B. Communications Systems (radios, 9-1-1, telephone, social media) 1-5:
   a. Potential defensive tactics:

C. Departmental Resources (swatting). 1-5:
   a. Potential defensive tactics:

D. Records Management Systems: 1-5:
   a. Potential defensive tactics:

Q3. Some consensus existed around the role that an increase in arrest/prosecution of hacktivists and cybercriminals may have in deterring these actors from targeting law enforcement agencies in the future. Please rank your level of agreement with your fellow experts (scale of 1-5) that this increase would deter future attacks if successful (assuming that such a task is attainable). Additionally, please describe in detail, tactics law enforcement agencies and their IT components could employ to increase the likelihood of arrest/prosecution of these cyber actors.

A. An increase in arrest and prosecution of hacktivists and other cybercriminals would likely deter future actors. 1-5:
    a. Tactics U.S., state, and local agencies could implement to increase the arrest and prosecution of cyber actors:

Q4. Two distinct themes emerged from Round 1 regarding significant barriers to law enforcement agencies protecting their IT systems. The first of these themes indicate that the factors listed below are each significant administrative, management driven barriers. Please indicate your level of agreement (1-5) that each of these serve as barriers in your experience. Next, describe tactics that could be employed by law enforcement agencies and their IT components to minimize the impact or remove these barriers to better position the agency to protect itself from the impact of hacktivism.

A. Budgetary Restraints. 1-5:
    a. Mitigation Tactics:

B. Staffing Challenges. 1-5:
    a. Mitigation Tactics:

C. Training Challenges (Having adequate expertise). 1-5:
    a. Mitigation Tactics:

D. Cyber Hygiene (Failure to patch systems, implement technical controls, etc.). 1-5:
    a. Mitigation Tactics:

E. Failure to obtain or act on cyber intelligence (indicators of compromise, news of active attack campaigns, etc.). 1-5:
    a. Mitigation Tactics:

Q5. The second theme regarding significant barriers to cyber defense for law enforcement agencies is the introduction (or lack of introduction) of cloud and other third-party services. While perspectives differed on the degree to which these services helped or hindered defensive efforts, a strong indication was given that the dependency of agencies on these commercial services and the ability to safely introduce them was a significant barrier. First, indicate your agreement with your peers that these services present defensive challenges (1-5). Next, describe in some detail what tactics agencies could employ to ensure that these services are implemented in a manner that contributes to the successful defense of the agency against a hacktivist attack.

A. The introduction of third-party services such as those offered by cloud service providers presents defensive challenges to agencies attempting to defend against hacktivist attacks. 1-5:
    a. Mitigation Tactics:

## APPENDIX C

## Round 3 Questionnaire

Delphi Study – Patrick J. Woods, Capella University
Round 3
Participant ID (to be completed by the researcher):

In Round 2, several themes from Round 1 were tested to gauge consensus among the panel members. Additionally, you were asked to provide specific tactics that could be used to mitigate challenges and contribute to a defensive model that may be employed by law enforcement agencies to protect against hacktivist attacks. In this round (3), you will be asked to examine the themes that have emerged from these rounds in the form of needs to be addressed by a cybersecurity defensive model. Once again, you will be asked to examine the theme and indicate your level of agreement with the position by selecting a rating on a scale of 1-5 (1 – Strongly disagree; 5 – Strongly Agree). Once complete consensus is reached, these themes will be utilized by the researcher combined with your recommendations on specific tactics tied to each to create a defensive model in response to the research question. Please remember that each of these needs is presented in the context of reducing the impact of a hacktivist attack on a law enforcement agency. If for whatever reason you strongly disagree with the position presented or feel strongly that something additional should be added, you will be afforded the opportunity to express these thoughts below each question.

### Theme 1

Media coverage, public sentiment and larger sociopolitical issues surrounding controversial law enforcement incidents are major contributors to a law enforcement agency being targeted by hacktivists. As a defensive tactic, law enforcement agencies should proactively work to manage the public message and public sentiment both ahead of, during, and following a controversial incident.

Please indicate your level of agreement with the position above (1-5):
Comments:

### Theme 2

Public-facing (internet-accessible) systems are at the greatest risk to be targeted by hacktivists and other cyber actors. Agencies should first focus their technical cybersecurity strategies on securing these most vulnerable systems.

Please indicate your level of agreement with the position above (1-5):
Comments:

**Theme 3**

With proper resources and legal changes, an increase in the arrest and prosecution of cyber threat actors would act as a deterrent to future potential hacktivists. Law enforcement agencies should advocate for changes to the law to increase the likelihood of successful arrest and prosecution, dedicate additional resources to cybercrime investigations, and consider restricting their own network traffic to IP addresses located within the United States or other extraditable jurisdictions.

Please indicate your level of agreement with the position above (1-5):
Comments:

**Theme 4**

Time, money, people, and skills represent the most significant challenges in law enforcement agency cyber defense. Agencies should focus administrative cybersecurity efforts on recruitment, retention, education, and budget allocations to improve defensive capabilities.

Please indicate your level of agreement with the position above (1-5):
Comments:

# APPENDIX D

## Email to Delphi Participants

Dear <Name and Title of Participant>,

I sincerely appreciate your participation in this Delphi study. The purpose of this study is to examine the perceptions and experiences of law enforcement technology experts like yourself, to develop consensus around the effectiveness of preventative measures undertaken by law enforcement agencies in order to mitigate the effects of hacktivism, and to predict future impacts of hacktivist actions on the operations of state and local law enforcement. At the conclusion of this study, the area of consensus will be used to develop a model to study for further study and refine defensive techniques employed by law enforcement agencies. Your participation in this study is highly valuable to both the law enforcement and academic communities by assisting in the development of a model that may be employed by other agencies and by expanding the overall body of knowledge in this area.

This study will consist of approximately three to four rounds of questionnaires, with the first round consisting of questions aimed at exposing themes which will be used to formulate questions for subsequent rounds. The study will conclude once adequate consensus is gauged. It is estimated that your participation in this study will take no more than 6-8 weeks to complete.

Please contact me at mocybersec@outlook.com if you have any questions or concerns.

Sincerely,

Patrick J. Woods