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

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

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-